DATA TERMINAL EQUIPMENT AND DATA RECORDING DEVICE

Publication number: JP2002366442

Publication date: 2002-12-20

Inventor: HORI YOSHIHIRO

Applicant: SANYO ELECTRIC CO

Classification:

- international: ***G06F12/14; G06F21/24; G06K19/073; H04L9/08; H04M11/00; H04N5/765; H04N5/907; H04N5/91; H04N7/167;*** **G06F12/14; G06F21/00; G06K19/073; H04L9/08; H04M11/00; H04N5/765; H04N5/907; H04N5/91; H04N7/167;** (IPC1-7): H04N5/765; H04N5/907; H04N5/91; G06F12/14; G06K19/073; H04L9/08; H04M11/00; H04N7/167

- European:

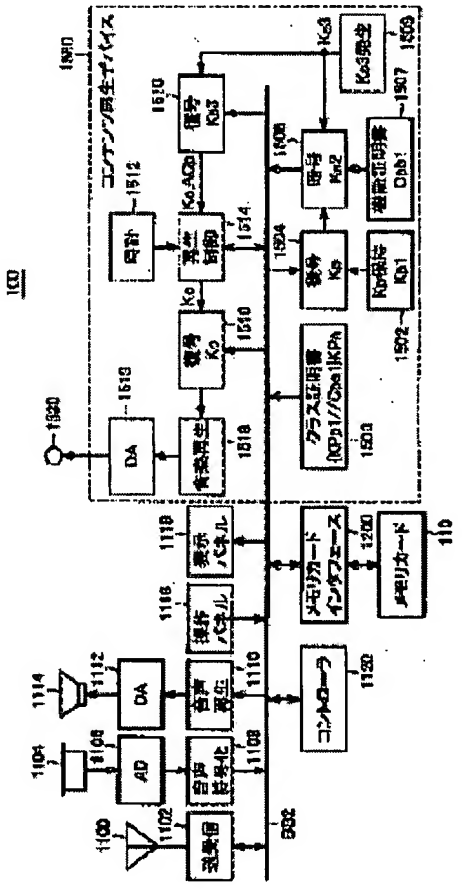
Application number: JP20010175036 20010611

Priority number(s): JP20010175036 20010611

Report a data error here

Abstract of **JP2002366442**

PROBLEM TO BE SOLVED: To provide a data recording device and data terminal equipment corresponding to this data recording device capable of preventing the transfer of any license key corresponding to encrypted contents data under reproduction control which can not be controlled by a reproducing terminal or encrypted contents data which can not be reproduced by the reproducing terminal to the terminal equipment. SOLUTION: A portable telephone set 100 is provided with a function certificate holding part 1507 so that a function certificate Cbp1 can be transmitted to a memory card 110. Then, when a function certified by the function certificate is made correspond to a function limited by reproduction control information ACp, the portable telephone set 100 acquires the license key Kc for decoding encrypted contents data Dc}Kc and the reproduction control information ACp from the memory card 110. A reproduction control part 1514 judges the validity/invalidity of the reproduction of the encrypted contents data Dc}Kc based on time information from a clock 1512 and a reproduction period included in the reproduction control information ACp.



Cited reference 3: 2002-366442

[0044] FIG. 2 is a diagram showing data for communication to be used and characteristics of information and the like in the data distribution system shown in FIG. 1.

[0045] First, the data to be distributed from a distribution server 10 will be described. Symbol Dc is content data such as music data. The content data Dc is encrypted so that the data can be decrypted with a license key Kc. Encrypted content data {Dc}Kc encrypted so that the data can be decrypted with the license key Kc is distributed in this form from the distribution server 10 to users of cellular phones 100, 102 and 104.

[0046] It is to be noted that, in the following description, notation {Y}X indicates that data Y is encrypted so that the data can be decrypted with a decryption key X.

[0047] Furthermore, copyright concerning the content data or additional information Dc-inf as plaintext information concerned with server access or the like is distributed from the distribution server 10 together with the encrypted content data. In addition, as license, the license key Kc, and license ID which is a control code to specify distribution of the license key or the like from the distribution server 10 are exchanged between the distribution server 10 and the cellular phones 100, 102 and 104. Furthermore, examples of the license include access control information ACm which is generated based on license purchase conditions AC including information such as a

content ID as a code to identify the content data Dc, a license number and a functional limitation determined in response to designation from a user side and which is information concerning a restriction on an access to the license in a recording device (a memory card); and reproduction control information ACp which is control information concerning reproduction in a data reproduction terminal.

[0048] Specifically, the access control information ACm is control information in a case where the license or the license key is output from the memory card, and includes limiting information concerning the number of reproducible times (the number of times to output the license key for the reproduction) and movement and duplicate of the license and the like.

[0049] The reproduction control information ACp is information which limits the reproduction, after a content reproduction circuit to reproduce the encrypted content data has received the license key. As shown in FIG. 3, the reproduction control information ACp includes flags FG1 to FG5 as reproduction limiting flags. The flag FG1 indicates reproduction speed change prohibition, the flag FG2 indicates whether or not edition is permitted, the flag FG3 indicates whether or not a region code is designated, the flag FG4 indicates whether or not a reproduction start date is designated, and the flag FG5 indicates whether or not a reproduction end date is designated. The reproduction

control information ACp further includes the corresponding region code in a case where the region code is designated, the corresponding reproduction start date in a case where the reproduction start date is designated, and the corresponding reproduction end date in a case where the reproduction end date is designated.

[0050] That is, the reproduction control information ACp includes an area 1 where the flags FG1 to FG5 are stored and an area 2 where actual data corresponding to the flags FG3 to FG5 is stored. The area 2 includes areas 21 to 23. In a case where the flag FG3 indicates that the region code is designated, in the area 21, a region code indicating a region where the encrypted content data can be reproduced is stored. In the area 22, the reproduction start date of the encrypted content data is stored in a case where the flag FG4 indicates that the reproduction start date is designated. In the area 23, the reproduction end date of the encrypted content data is stored in a case where the flag FG5 indicates that the reproduction end date is designated.

[0051] In the flags FG1 to FG5, "1" or "0" is stored. When the flag indicates "1", it is meant that the flag is active and that a limitation due to a reproducing limitation corresponding to the flag is imposed. When the flag indicates "0", it is meant that the flag is negative and that any limitation due to the reproducing limitation corresponding to the flag is not imposed. Specifically, when "1" is stored in the flag FG1, the change prohibition

of the reproduction speed is meant. When "0" is stored, it is meant that the reproduction speed may be changed. When "1" is stored in the flag FG2, the permission of the edition is meant. When "0" is stored, the prohibition of the edition is meant. Furthermore, when "1" is stored in the flag FG3, it is meant that the region code capable of reproducing the encrypted content data is designated. When "0" is stored, it is meant that the region code capable of reproducing the encrypted content data is not designated, that is, all the areas are designated. In addition, when "1" is stored in the flag FG4, it is meant that the reproduction start date when the reproduction of the encrypted content data can be started is designated. When "0" is stored, it is meant that the reproduction start date when the reproduction of the encrypted content data can be started is not designated. Moreover, when "1" is stored in the flag FG5, it is meant that the reproduction end date when the encrypted content data cannot be reproduced any more is designated. When "0" is stored, it is meant that the reproduction end date when the encrypted content data cannot be reproduced any more is not designated.

[0052] Therefore, the reproduction circuit of the encrypted content data searches for the flags FG1 to FG5 of the reproduction control information ACp. Moreover, the reproduction circuit reproduces the encrypted content data without changing the speed in a case where "1" is stored in the flag FG1, and changes the speed to reproduce the

encrypted content data in a case where "0" is not stored. The reproduction circuit edits the encrypted content data in response to an instruction from a user in a case where "1" is stored in the flag FG2, and does not edit the encrypted content data in a case where "0" is stored. Furthermore, the reproduction circuit judges whether or not a region where the encrypted content data is to be reproduced is a region stored in the area 21 in a case where "1" is stored in the flag FG3, reproduces the encrypted content data in a case where it is judged that the region where the encrypted content data is to be reproduced is the region stored in the area 21, and does not reproduce the encrypted content data in a case where the region is a region other than the region stored in the area 21 and the encrypted content data is to be reproduced. Moreover, the reproduction circuit reproduces the encrypted content data without judging whether or not the region where the encrypted content data is to be reproduced is the region stored in the area, in a case where "0" is stored in the flag FG3.

[0053] Moreover, the reproduction circuit refers to the reproduction start date stored in the area 22 in a case where "1" is stored in the flag FG4, reproduces the encrypted content data in a case where the reproduction start date is reached, and does not reproduce the encrypted content data in a case where the reproduction start date is not reached. Furthermore, the reproduction circuit refers to the reproduction end date stored in the area 23 in a case

where "1" is stored in the flag FG5, ends the reproduction of the encrypted content data in a case where the reproduction end date is reached, and continues the reproduction of the encrypted content data in a case where the reproduction end date is not reached.

[0054] It is to be noted that, in the present invention, either or the reproduction start date and the reproduction end date is designated in some case. That is, there is a case where the only reproduction start date is designated and the reproduction end date is not designated or a case where the reproduction start date is not designated and the reproduction end date is designated. In the former case, the reproduction end date is not stored in the area 23. In the latter case, the reproduction start date is not stored in the area 22.

[0055] In the present invention, especially, the reproduction start date or the reproduction end date is set to the reproduction control information ACp, and time of the reproduction of the encrypted content data is limited using the reproduction start date or the reproduction end date. It is indicated that the areas 21 to 23 constituting the area 2 are constantly secured, but the areas may be omitted at a time when the corresponding flags FG3 to FG5 are negative or "0".

~~図11~~ F1g1

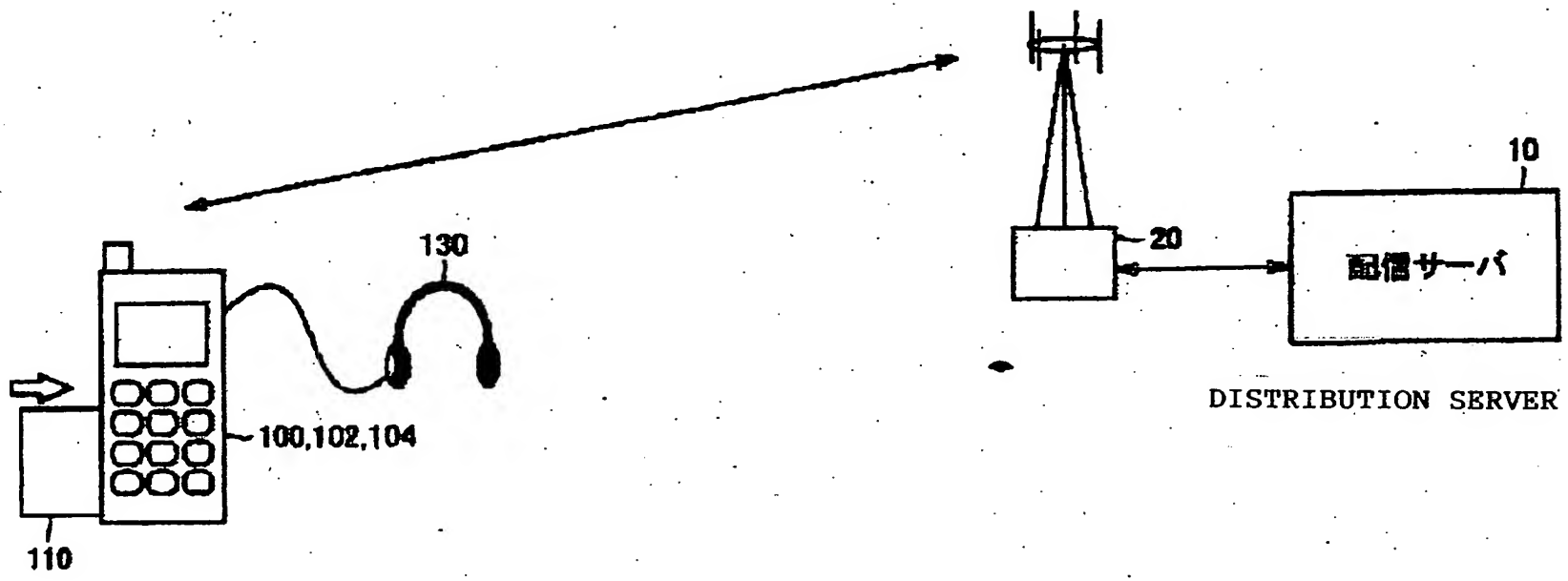


FIG. 2

Symbol	Type	Attribute	Characteristics
Do	Content data	Inherent in contents	Ex.: Music data, reading data, teaching material data, image data, encrypted content data which can be decrypted with Kc and which is stored as {Dc}Kc and which is retained in memory card
Dc-inf	Additional information	Inherent in contents	Plaintext data accompanying Dc
Ko	License	Inherent in contents	License Decryption key to decrypt encrypted content data
ACm/ACp	License	Inherent in contents	Limit information Limitation matters concerning reproduction and handling of license
Content ID	License	Inherent in contents	Control code to specify contents
License ID	License	Inherent in contents	Control code to specify license
License	License	Inherent in license	Generic term of Kc + ACm + ACp + Content ID + License ID

FIG. 3

ACP flag

Reproduction limiting flag

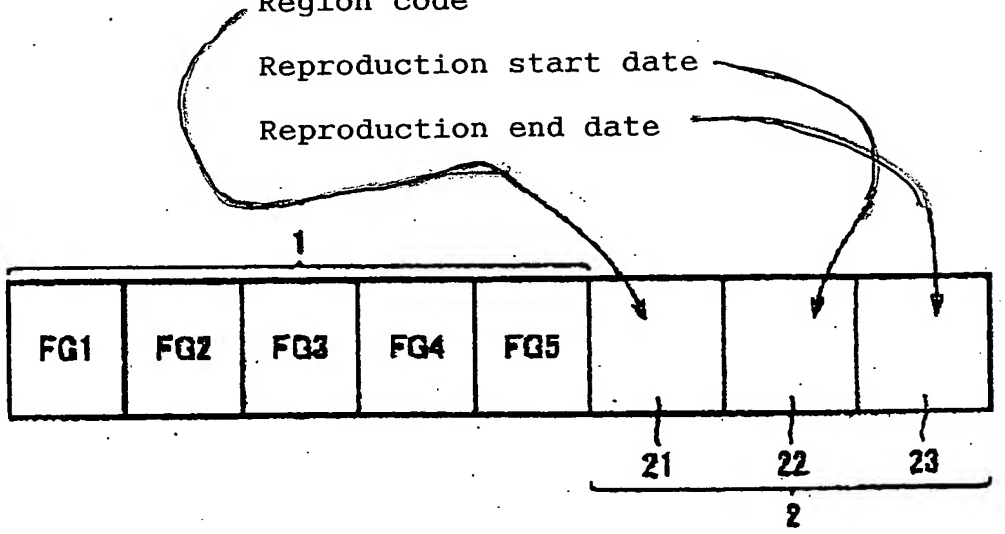
FG1: Reproduction speed change prohibition

FG2: Whether or not edition is permitted

FG3: Whether or not region code is designated

FG4: Whether or not reproduction start date is designated

FG5: Whether or not reproduction end date is designated



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－366442
（P2002－366442A）
(43)公開日　平成14年12月20日(2002.12.20)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード(参考)
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｆ	５Ｂ０１７
			３２０Ｂ	５Ｂ０３５
Ｇ０６Ｋ　19/073		Ｈ０４Ｍ　11/00	３０２	５Ｃ０５２
Ｈ０４Ｌ　9/08		Ｈ０４Ｎ　5/907	Ｂ	５Ｃ０５３
Ｈ０４Ｍ　11/00	３０２	Ｇ０６Ｋ　19/00	Ｐ	５Ｃ０６４

審査請求　未請求　請求項の数15　ＯＬ　（全 33 頁）　最終頁に続く

(21)出願番号　特願2001－175036(P2001－175036)

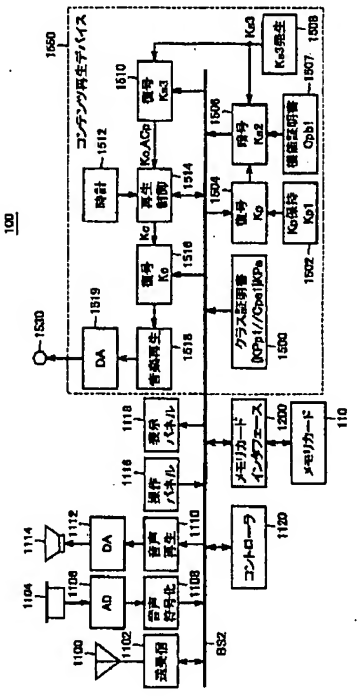
(22)出願日　平成13年６月11日(2001.6.11)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(72)発明者　堀　吉宏
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(74)代理人　100064746
弁理士　深見　久郎　（外３名）

最終頁に続く

(54)【発明の名称】　データ端末装置およびデータ記録装置

(57)【要約】
【課題】　再生端末で制御できない再生制御を受ける暗号化コンテンツデータや再生端末で再生できない暗号化コンテンツデータに対するライセンス鍵を端末装置に提供しないデータ記録装置およびそれに対応したデータ端末装置を提供する。
【解決手段】　携帯電話機１００は、機能証明書保持部１５０７を備え、機能証明書Ｃｐｂ１をメモリカード１１０へ送信する。そして、機能証明書によって証明される機能が再生制御情報ＡＣｐによって制限される機能に対応しているとき、携帯電話機１００は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号するためのライセンス鍵Ｋｃと再生制御情報ＡＣｐをメモリカード１１０から取得する。再生制御部１５１４は、時計１５１２からの時間情報と再生制御情報ＡＣｐに含まれる再生期限とに基づいて暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの再生の可否を判断する。



1

【特許請求の範囲】

【請求項１】　暗号化コンテンツデータと、前記暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスとをデータ記録装置から取得して前記暗号化コンテンツデータを復号および再生するデータ端末装置であって、

前記データ記録装置との間のデータのやり取りを制御するインタフェースと、

前記暗号化コンテンツデータを前記ライセンス鍵によって復号および再生するコンテンツ再生手段と、

前記コンテンツ再生手段における再生機能を証明する機能証明書を保持する機能証明書保持部と、

指示を入力するためのキー操作部と、

制御手段とを備え、

前記制御手段は、前記キー操作部を介して入力された前記暗号化コンテンツデータの再生要求に応じて前記機能証明書を前記インタフェースを介して前記データ記録装置へ送信し、前記機能証明書によって証明された機能が前記ライセンスに含まれる再生制限情報により制限しようとする機能に対応しているとき、前記インタフェースを介して前記データ記録装置から前記暗号化コンテンツデータおよび前記ライセンスを受信し、その受信した暗号化コンテンツデータおよびライセンスを前記コンテンツ再生手段に与える、データ端末装置。

【請求項２】　データを前記データ記録装置と送受信するときのセキュリティレベルを証明するクラス証明書を保持するクラス証明書保持部をさらに備え、

前記制御手段は、前記再生要求に応じて前記クラス証明書を前記インタフェースを介して前記データ記録装置へ送信し、前記データ記録装置において前記クラス証明書が認証されると、前記機能証明書を前記データ記録装置へ送信する、請求項１に記載のデータ端末装置。

【請求項３】　前記機能証明書保持部は、前記クラス証明書に含まれる公開暗号鍵によって復号可能な暗号化された機能証明書を保持する、請求項２に記載のデータ端末装置。

【請求項４】　前記制御手段は、前記機能証明書を前記クラス証明書と同時に前記データ記録装置へ送信する、請求項３に記載のデータ端末装置。

【請求項５】　前記データ記録装置との通信を特定するためのセッション鍵を生成するセッション鍵生成手段と、

前記セッション鍵によってデータを暗号化する暗号処理手段と、

前記セッション鍵によって暗号化された暗号化データを復号する復号処理手段とをさらに備え、

前記暗号化コンテンツデータおよび前記ライセンスを前記データ記録装置から取得するとき、

前記セッション鍵生成手段は、前記データ記録装置との通信を特定するための第１のセッション鍵を生成し、

2

前記暗号処理手段は、前記機能証明書および前記第１のセッション鍵を、前記データ記録装置から受取った第２のセッション鍵によって暗号化し、

前記制御手段は、前記第２のセッション鍵によって暗号化された前記機能証明書および前記第１のセッション鍵を前記インタフェースを介して前記データ記録装置へ送信する、請求項２から請求項４のいずれか１項に記載のデータ端末装置。

【請求項６】　前記制御手段は、さらに、前記第１のセッション鍵によって暗号化された前記再生制限情報および前記ライセンス鍵を前記データ記録装置から受信して前記復号処理手段に与え、前記復号処理手段により復号された前記再生制限情報によって前記暗号化コンテンツデータの再生が制限されていないとき前記暗号化コンテンツデータおよび前記ライセンス鍵を前記コンテンツ再生手段に与える、請求項５に記載のデータ端末装置。

【請求項７】　リアルタイムに日時情報を更新する時計部をさらに備え、

前記再生制限情報は、前記暗号化コンテンツデータの再生期間を制限する期間制限情報を含み、

前記制御手段は、前記時計部からの日時情報と前記期間制限情報とに基づいて前記暗号化コンテンツデータの再生期間内か否かを判定する、請求項６に記載のデータ端末装置。

【請求項８】　暗号化コンテンツデータと、前記暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスとを記録するデータ記録装置であって、

前記暗号化コンテンツデータおよび前記ライセンスを記憶する記憶手段と、

前記暗号化コンテンツデータを前記ライセンスによって復号および再生するデータ再生装置との間でデータのやり取りを行なうインタフェースと、

制御手段とを備え、

前記制御手段は、前記データ再生装置の機能を証明する機能証明書を前記インタフェースを介して受取り、その受取った機能証明書によって証明された機能が前記ライセンスに含まれる再生制限情報により制限しようとする機能に対応しているとき、前記暗号化コンテンツデータおよび前記ライセンスを前記記憶手段から読出して前記インタフェースを介して前記データ再生装置へ送信する、データ記録装置。

【請求項９】　前記データ再生装置に固有な公開暗号鍵によって暗号化されたデータを秘密復号鍵によって復号する復号処理手段をさらに備え、

前記制御手段は、前記公開暗号鍵によって暗号化された機能証明書を前記インタフェースを介して受取り、前記暗号化された機能証明書を前記復号処理手段に与え、復号された機能証明書を前記復号処理手段から受取る、請求項８に記載のデータ記録装置。

【請求項１０】　公開認証鍵によって暗号化されたデー

タを前記公開認証鍵によって復号する第１の復号処理手段と、
前記データ再生装置に固有な公開暗号鍵によって暗号化されたデータを秘密復号鍵によって復号する第２の復号処理手段とをさらに備え、
前記制御手段は、前記公開認証鍵によって復号可能な暗号化されたクラス証明書と、前記公開暗号鍵によって復号可能な暗号化された機能証明書とを前記インタフェースを介して同時に受取り、前記暗号化されたクラス証明書を前記第１の復号処理手段に与え、前記暗号化された機能証明書を前記第２の復号処理手段に与え、復号されたクラス証明書および機能証明書を受取る、請求項８に記載のデータ記録装置。
【請求項１１】　前記データ再生装置との通信を特定するためのセッション鍵を生成するセッション鍵生成手段と、
前記セッション鍵によって暗号化されたデータを復号するもう１つの復号処理手段と、
前記データ再生装置に固有な公開暗号鍵によってデータを暗号化する暗号処理手段とをさらに備え、
前記機能証明書を受信するとき、
前記セッション鍵生成手段は、前記データ再生装置との通信を特定するための第１のセッション鍵を生成し、
前記暗号処理手段は、前記公開暗号鍵によって前記第１のセッション鍵を暗号化し、
前記制御手段は、前記公開暗号鍵によって暗号化された第１のセッション鍵を前記インタフェースを介して前記データ再生装置へ送信し、前記第１のセッション鍵によって暗号化された機能証明書を前記インタフェースを介して受信して前記もう１つの復号処理手段に与え、復号された機能証明書を前記もう１つの復号処理手段から受取り、
前記もう１つの復号処理手段は、前記暗号化された機能証明書を前記第１のセッション鍵によって復号する、請求項８から請求項１０のいずれか１項に記載のデータ記録装置。
【請求項１２】　前記セッション鍵によってデータを暗号化するもう１つの暗号処理手段をさらに備え、
前記制御手段は、前記機能証明書によって証明された機能が前記ライセンスに含まれる再生制限情報により制限しようとする機能に対応していると判断すると、前記記憶手段から読出した前記ライセンス鍵および前記再生制限情報を前記もう１つの暗号処理手段に与え、前記データ再生装置において生成された第２のセッション鍵によって暗号化されたライセンス鍵および再生制限情報を前記インタフェースを介して前記データ再生装置へ送信し、
前記もう１つの暗号処理手段は、前記第２のセッション鍵によって前記ライセンス鍵および前記再生制限情報を暗号化する、請求項１１に記載のデータ記録装置。
【請求項１３】　前記制御手段は、前記データ再生装置が前記機能証明書を保持しないときデフォルト値を前記機能証明書として受理する、請求項８から請求項１２のいずれか１項に記載のデータ記録装置。
【請求項１４】　前記再生制限情報は、
前記暗号化コンテンツデータの再生を開始できる再生開始日時と、
前記暗号化コンテンツデータの再生ができなくなる再生終了日時とのいずれか一方を少なくとも含む、請求項８から請求項１３のいずれか１項に記載のデータ記録装置。
【請求項１５】　前記再生制限情報は、前記暗号化コンテンツデータを再生可能な地域を示す地域コードをさらに含む、請求項１４に記載のデータ記録装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムを用いて取得された暗号化データを復号および再生する際に、暗号化データの再生制限情報の内容に応じた暗号化データの再生を実現するデータ端末装置およびデータ記録装置に関するものである。
【０００２】
【従来の技術】近年、インターネット等のデジタル情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。
【０００３】このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。
【０００４】したがって、このようなデジタル情報通信網上において音楽データや画像データ等の著作者の権利が存在するコンテンツが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。
【０００５】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。
【０００６】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽デー

タのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【０００７】しかも、ＣＤからＭＤへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【０００８】このような事情からも、音楽データや画像データ等のコンテンツデータをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【０００９】この場合、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【００１０】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【００１１】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【００１２】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話機に装着する。携帯電話機は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【００１３】このように、携帯電話機のユーザは、ダウンロード端末としての携帯電話機を用いて暗号化コンテンツデータと暗号化コンテンツデータを再生するために必要なライセンス鍵を含むライセンスを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。そして、暗号化コンテンツデータを復号および再生するために必要なライセンスは、ライセンス鍵の他に暗号化コンテンツデータの再生に対して制限を加える再生制限情報を含み、暗号化コンテンツデータを再生するデータ端末装置としての携帯電話機は、この再生制御情報に従って暗号化コンテンツデータの再生の際に制限を加える。

【００１４】

【発明が解決しようとする課題】しかし、このようなシステムにおいては、データ記録装置であるメモリカードが中心となってユーザ側でのライセンスの管理を行なっているにも拘わらず、ライセンス鍵を安全に管理しているデータ記録装置は、再生端末による制限が必ず実施されているかを判断することができないという問題があった。

【００１５】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、再生端末で制御できない再生制御を受ける暗号化コンテンツデータや再生端末で再生できない暗号化コンテンツデータに対するライセンス鍵を端末装置に提供しないデータ記録装置およびそれに対応したデータ端末装置を提供することである。

【００１６】

【課題を解決するための手段】この発明によれば、データ端末装置は、暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスとをデータ記録装置から取得して暗号化コンテンツデータを復号および再生するデータ端末装置であって、データ記録装置との間のデータのやり取りを制御するインタフェースと、暗号化コンテンツデータをライセンス鍵によって復号および再生するコンテンツ再生手段と、コンテンツ再生手段における再生機能を証明する機能証明書を保持する機能証明書保持部と、指示を入力するためのキー操作部と、制御手段とを備え、制御手段は、キー操作部を介して入力された暗号化コンテンツデータの再生要求に応じて機能証明書をインタフェースを介してデータ記録装置へ送信し、機能証明書によって証明された機能がライセンスに含まれる再生制限情報により制限しようとする機能に対応しているとき、インタフェースを介してデータ記録装置から暗号化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータおよびライセンスをコンテンツ再生手段に与える。

【００１７】好ましくは、データ端末装置は、データを前記データ記録装置と送受信するときのセキュリティレ

ベルを証明するクラス証明書を保持するクラス証明書保持部をさらに備え、制御手段は、再生要求に応じてクラス証明書をインタフェースを介してデータ記録装置へ送信し、データ記録装置においてクラス証明書が認証されると、機能証明書を前記データ記録装置へ送信する。

【００１８】好ましくは、機能証明書保持部は、クラス証明書に含まれる公開暗号鍵によって復号可能な暗号化された機能証明書を保持する。

【００１９】好ましくは、制御手段は、機能証明書をクラス証明書と同時にデータ記録装置へ送信する。

【００２０】好ましくは、データ端末装置は、データ記録装置との通信を特定するためのセッション鍵を生成するセッション鍵生成手段と、セッション鍵によってデータを暗号化する暗号処理手段と、セッション鍵によって暗号化された暗号化データを復号する復号処理手段とをさらに備え、暗号化コンテンツデータおよびライセンスをデータ記録装置から取得するとき、セッション鍵生成手段は、データ記録装置との通信を特定するための第１のセッション鍵を生成し、暗号処理手段は、機能証明書および第１のセッション鍵を、データ記録装置から受取った第２のセッション鍵によって暗号化し、制御手段は、第２のセッション鍵によって暗号化された機能証明書および第１のセッション鍵をインタフェースを介してデータ記録装置へ送信する。

【００２１】好ましくは、制御手段は、さらに、第１のセッション鍵によって暗号化された再生制限情報およびライセンス鍵をデータ記録装置から受信して復号処理手段に与え、復号処理手段により復号された再生制限情報によって暗号化コンテンツデータの再生が制限されていないとき暗号化コンテンツデータおよびライセンス鍵をコンテンツ再生手段に与える。

【００２２】好ましくは、データ端末装置は、リアルタイムに日時情報を更新する時計部をさらに備え、再生制限情報は、暗号化コンテンツデータの再生期間を制限する期間制限情報を含み、制御手段は、時計部からの日時情報と期間制限情報とに基づいて暗号化コンテンツデータの再生期間内か否かを判定する。

【００２３】また、この発明によれば、データ記録装置は、暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスとを記録するデータ記録装置であって、暗号化コンテンツデータおよびライセンスを記憶する記憶手段と、暗号化コンテンツデータをライセンスによって復号および再生するデータ再生装置との間でデータのやり取りを行なうインタフェースと、制御手段とを備え、制御手段は、データ再生装置の機能を証明する機能証明書をインタフェースを介して受取り、その受取った機能証明書によって証明された機能がライセンスに含まれる再生制限情報により制限しようとする機能に対応しているとき、暗号化コンテンツデータおよびライセンスを記憶手段から読出してインタフェースを介してデータ再生装置へ送信する。

【００２４】好ましくは、データ記録装置は、データ再生装置に固有な公開暗号鍵によって暗号化されたデータを秘密復号鍵によって復号する復号処理手段をさらに備え、制御手段は、公開暗号鍵によって暗号化された機能証明書をインタフェースを介して受取り、暗号化された機能証明書を復号処理手段に与え、復号された機能証明書を復号処理手段から受取る。

【００２５】好ましくは、データ記録装置は、公開認証鍵によって暗号化されたデータを公開認証鍵によって復号する第１の復号処理手段と、データ再生装置に固有な公開暗号鍵によって暗号化されたデータを秘密復号鍵によって復号する第２の復号処理手段とをさらに備え、制御手段は、公開認証鍵によって復号可能な暗号化されたクラス証明書と、公開暗号鍵によって暗号化された機能証明書とをインタフェースを介して同時に受取り、暗号化されたクラス証明書を第１の復号処理手段に与え、暗号化された機能証明書を第２の復号処理手段に与え、復号されたクラス証明書および機能証明書を受取る。

【００２６】好ましくは、データ記録装置は、データ再生装置との通信を特定するためのセッション鍵を生成するセッション鍵生成手段と、セッション鍵によって暗号化されたデータを復号するもう１つの復号処理手段と、データ再生装置に固有な公開暗号鍵によってデータを暗号化する暗号処理手段とをさらに備え、機能証明書を受信するとき、セッション鍵生成手段は、データ再生装置との通信を特定するための第１のセッション鍵を生成し、暗号処理手段は、公開暗号鍵によって第１のセッション鍵を暗号化し、制御手段は、公開暗号鍵によって暗号化された第１のセッション鍵をインタフェースを介してデータ再生装置へ送信し、第１のセッション鍵によって暗号化された機能証明書をインタフェースを介して受信してもう１つの復号処理手段に与え、復号された機能証明書をもう１つの復号処理手段から受取り、もう１つの復号処理手段は、暗号化された機能証明書を第１のセッション鍵によって復号する。

【００２７】好ましくは、セッション鍵によってデータを暗号化するもう１つの暗号処理手段をさらに備え、制御手段は、機能証明書によって証明された機能がライセンスに含まれる再生制限情報により制限しようとする機能に対応していると判断すると、記憶手段から読出したライセンス鍵および再生制限情報をもう１つの暗号処理手段に与え、データ再生装置において生成された第２のセッション鍵によって暗号化されたライセンス鍵および再生制限情報をインタフェースを介してデータ再生装置へ送信し、もう１つの暗号処理手段は、第２のセッション鍵によってライセンス鍵および再生制限情報を暗号化する。

【００２８】好ましくは、制御手段は、データ再生装置が機能証明書を保持しないときデフォルト値を機能証明

番として受理する。

【００２９】好ましくは、再生制限情報は、暗号化コンテンツデータの再生を開始できる再生開始日時と、暗号化コンテンツデータの再生ができなくなる再生終了日時とのいずれか一方を少なくとも含む。

【００３０】好ましくは、再生制限情報は、暗号化コンテンツデータを再生可能な地域を示す地域コードをさらに含む。

【００３１】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００３２】［実施の形態１］図１は、本発明によるデータ記録装置が暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのライセンスを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

【００３３】なお、以下では携帯電話網を介して音楽データをユーザの携帯電話機に装着されたメモリカード１１０に配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても適用することが可能なものである。

【００３４】図１を参照して、配信キャリア２０は、自己の携帯電話網を通じて得た、ユーザからの配信要求（配信リクエスト）を配信サーバ１０に中継する。音楽データを管理する配信サーバ１０は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機１００，１０２，１０４に装着されたメモリカード１１０が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して著作権を保護するために所定の暗号方式により音楽データ（以下、コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア２０である携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報として暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスを与える。

【００３５】配信キャリア２０は、自己の携帯電話網を通じて配信要求を送信した携帯電話機１００，１０２，１０４に装着されたメモリカード１１０に対して、携帯電話網および携帯電話機１００，１０２，１０４を介して暗号化コンテンツデータとライセンスとを配信する。

【００３６】図１においては、たとえば携帯電話ユーザの携帯電話機１００，１０２，１０４には、着脱可能なメモリカード１１０が装着される構成となっている。メモリカード１１０は、携帯電話機１００，１０２，１０４により受信された暗号化コンテンツデータを受取り、著作権を保護するために行なわれた暗号化を復号した上で、携帯電話機１００，１０２，１０４に含まれる音楽再生部（図示せず）に与える。

【００３７】さらに、たとえば携帯電話ユーザは、携帯電話機１００，１０２，１０４に接続したヘッドホーン１３０等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【００３８】このような構成とすることで、まず、メモリカード１１０を利用しないと、配信サーバ１０からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【００３９】しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００４０】したがって、図１に示すデータ配信システムにおいては、携帯電話機１００に装着されたメモリカード１１０は、携帯電話網を介して配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信することができる。

【００４１】図１に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話機のユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信におけるライセンスを配信するための方式であり、さらに第２には、コンテンツデータを暗号化する方式そのものであり、さらに、第３には、このような再生可能な状態でのコンテンツデータの無断コピーを防止するための著作権保護を実現する構成である。

【００４２】本発明の実施の形態においては、特に、配信、および再生の各処理の発生時において、これらの暗号化コンテンツデータを再生するために必要なライセンスの移動先に対する認証およびチェック機能を充実させ、非認証の記録装置およびデータ再生端末（暗号化コンテンツデータを復号して再生できる再生端末を携帯電話機とも言う。以下同じ）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【００４３】なお、以下の説明においては、配信サーバ１０から、各携帯電話機に暗号化コンテンツデータまたはそのライセンスを伝送する処理を「配信」と称することとする。

【００４４】図２は、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【００４５】まず、配信サーバ１０より配信されるデータについて説明する。Ｄｃは、音楽データ等のコンテンツデータである。コンテンツデータＤｃは、ライセンス

鍵Ｋｃで復号可能な暗号化が施される。ライセンス鍵Ｋｃによって復号可能な暗号化が施された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃがこの形式で配信サーバ１０より携帯電話機１００，１０２，１０４のユーザに配布される。

【００４６】なお、以下においては、｛Ｙ｝Ｘという表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。

【００４７】さらに、配信サーバ１０からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Ｄｃ－ｉｎｆが配布される。また、ライセンスとして、ライセンス鍵Ｋｃ、配信サーバ１０からのライセンス鍵等の配信を特定するための管理コードであるライセンスＩＤが配信サーバ１０と携帯電話機１００，１０２，１０４との間でやり取りされる。さらに、ライセンスとしては、コンテンツデータＤｃを識別するためのコードであるコンテンツＩＤや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ＡＣに基づいて生成される、記録装置（メモリカード）におけるライセンスのアクセスに対する制限に関する情報であるアクセス制御情報ＡＣｍおよびデータ再生端末における再生に関する制御情報である再生制御情報ＡＣｐ等が存在する。

【００４８】具体的には、アクセス制御情報ＡＣｍは、メモリカードからのライセンスまたはライセンス鍵を外部に出力するに当っての制御情報であり、再生可能回数（再生のためにライセンス鍵を出力する回数）、ライセンスの移動・複製に関する制限情報などがある。

【００４９】再生制御情報ＡＣｐは、暗号化コンテンツデータを再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生を制限する情報である。図３を参照して、再生制御情報ＡＣｐは、再生制限フラグとしてフラグＦＧ１～ＦＧ５を含む。フラグＦＧ１は、再生速度変更禁止を示し、フラグＦＧ２は、編集可否を示し、フラグＦＧ３は、地域コードの指定有無を示し、フラグＦＧ４は、再生開始日時の指定有無を示し、フラグＦＧ５は、再生終了日時の指定有無を示す。再生制御情報ＡＣｐは、さらに、地域コードの指定が有る場合、それに対応する地域コードと、再生開始日時の指定が有る場合、それに対応する再生開始日時と、再生終了日時の指定がある場合、それに対応する再生終了日時とを含む。

【００５０】すなわち、再生制御情報ＡＣｐは、フラグＦＧ１～ＦＧ５が格納された領域１と、フラグＦＧ３～ＦＧ５に対応する実データが格納された領域２とから成る。領域２は、領域２１～２３から成る。領域２１は、フラグＦＧ３において地域コードの指定がある場合に、暗号化コンテンツデータの再生が可能な地域を示す地域コードが格納される。領域２２は、フラグＦＧ４において再生開始日時の指定がある場合に、暗号化コンテンツデータの再生開始日時が格納される。領域２３は、フラグＦＧ５において再生終了日時の指定がある場合に、暗号化コンテンツデータの再生終了日時が格納される。

【００５１】フラグＦＧ１～ＦＧ５には、「１」または「０」が格納される。フラグが「１」の場合には、そのフラグはアクティブであって、そのフラグに対応した再生制限による制限を受けることを意味し、フラグが「０」の場合には、そのフラグがネガティブであって、そのフラグに対応した再生制限による制限を受けないことを意味する。具体的には、フラグＦＧ１に「１」が格納された場合、再生速度の変更禁止を意味し、「０」が格納された場合、再生速度を変更しても良いことを意味する。また、フラグＦＧ２に「１」が格納された場合、編集の許可を意味し、「０」が格納された場合、編集の禁止を意味する。さらに、フラグＦＧ３に「１」が格納された場合、暗号化コンテンツデータを再生できる地域コードの指定が有ることを意味し、「０」が格納された場合、暗号化コンテンツデータを再生できる地域コードの指定が無い、すなわち、全領域指定であることを意味する。また、さらに、フラグＦＧ４に「１」が格納された場合、暗号化コンテンツデータの再生を開始できる再生開始日時の指定が有ることを意味し、「０」が格納された場合、暗号化コンテンツデータの再生を開始できる再生開始日時の指定が無いことを意味する。また、さらに、フラグＦＧ５に「１」が格納された場合、暗号化コンテンツデータの再生ができなくなる再生終了日時の指定が有ることを意味し、「０」が格納された場合、暗号化コンテンツデータの再生ができなくなる再生終了日時の指定が無いことを意味する。

【００５２】したがって、暗号化コンテンツデータの再生回路は、再生制御情報ＡＣｐのフラグＦＧ１～ＦＧ５を検索する。そして、再生回路は、フラグＦＧ１において「１」が格納されていれば、速度を変更せずに暗号化コンテンツデータを再生し、「０」が格納されていなければ速度を変更して暗号化コンテンツデータを再生する。また、再生回路は、フラグＦＧ２に「１」が格納されていれば、ユーザからの指示により暗号化コンテンツデータの編集を行ない、「０」が格納されていれば暗号化コンテンツデータの編集を行なわない。さらに、再生回路は、フラグＦＧ３に「１」が格納されていれば、暗号化コンテンツデータを再生しようとする地域が領域２１に格納された地域であるか否かを判定し、暗号化コンテンツデータを再生しようとする地域が領域２１に格納された地域であれば暗号化コンテンツデータの再生を行ない、領域２１に格納された地域以外で暗号化コンテンツデータを再生しようとしているときは暗号化コンテンツデータの再生を行なわない。そして、再生回路は、フラグＦＧ３に「０」が格納されていれば、暗号化コンテンツデータを再生しようとしている地域の判定を行なわ

ずに暗号化コンテンツデータの再生を行なう。

【００５３】また、さらに、再生回路は、フラグＦＧ４に「１」が格納されていれば、領域２２に格納された再生開始日時を参照し、その再生開始日時に達していれば暗号化コンテンツデータの再生を行ない、再生開始日時に達していなければ暗号化コンテンツデータの再生を行なわない。また、さらに、再生回路は、フラグＦＧ５に「１」が格納されていれば、領域２３に格納された再生終了日時を参照し、その再生終了日時に達していれば暗号化コンテンツデータの再生を終了し、再生終了日時に達していなければ暗号化コンテンツデータの再生を続行する。

【００５４】なお、本発明においては、再生開始日時および再生終了日時のうちいずれか一方のみが指定される場合もある。すなわち、再生開始日時のみが指定され、再生終了日時が指定されていない場合、または再生開始日時が指定されず、再生終了日時が指定されている場合がある。前者の場合、領域２３には再生終了日時が格納されず、後者の場合、領域２２には再生開始日時が格納されない。

【００５５】本発明においては、特に、再生開始日時または再生終了日時を再生制御情報ＡＣｐに設定し、再生開始日時または再生終了日時を用いて暗号化コンテンツデータの再生を時間的に制限する。また、領域２を構成する領域２１～２３は、常に確保されているように示されているが、それぞれに対応するフラグＦＧ３～ＦＧ５がネガティブ「０」の時には省略するように構成してもよい。

【００５６】再び、図２を参照して、ライセンスＩＤと、コンテンツＩＤと、ライセンス鍵Ｋｃと、アクセス制御情報ＡＣｍと、再生制御情報ＡＣｐとを併せて、以後、ライセンスと総称することとする。

【００５７】また、以降では、簡単化のためアクセス制御情報ＡＣｍは、再生回数の制限を行なう制御情報である再生回数（０：再生不可、１～２５４：再生可能回数、２５５：制限無し）、ライセンスの移動および複製を制限する移動・複製フラグ（０：移動複製禁止、１：移動のみ可、２：移動複製可）の２項目とする。

【００５８】図４は、図１に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【００５９】データ再生端末内のコンテンツ再生デバイス、およびメモリカードには固有の公開暗号鍵ＫＰｐｙおよびＫＰｍｗがそれぞれ設けられ、公開暗号鍵ＫＰｐｙおよびＫＰｍｗはコンテンツ再生回路に固有の秘密復号鍵Ｋｐｙおよびメモリカードに固有の秘密復号鍵Ｋｍｗによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、メモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【００６０】また、コンテンツ再生デバイスのクラス証明書としてＣｐａｙが設けられ、メモリカードのクラス証明書としてＣｍｗが設けられる。これらのクラス証明書は、コンテンツ再生デバイス、およびメモリカードのクラスごとに異なる情報を有する。

【００６１】さらに、コンテンツ再生デバイスの機能証明書としてＣｐｂｉが設けられる。この機能証明書は、コンテンツ再生デバイスが、再生制御情報ＡＣｐによって制限可能な機能を備えるか否かを示すものである。すなわち、再生制御情報ＡＣｐとして、再生開始日時または再生終了日時を設定した場合、コンテンツ再生デバイスは、暗号化コンテンツデータを再生する際の日時が、設定された再生開始日時または再生終了日時の条件を満たすか否かを判定する必要がある。そうすると、再生制御情報ＡＣｐとして再生開始日時または再生終了日時が設定されている暗号化コンテンツデータの再生が可能なコンテンツ再生デバイスは、時間を判定する機能を備えたコンテンツ再生デバイスである。したがって、コンテンツ再生デバイスのクラスごとに、時間の判定機能の有無が機能証明書Ｃｐｂｉに記載されている。

【００６２】これらのコンテンツ再生デバイスのクラス公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｐｙ／／Ｃｐａｙ｝ＫＰａの形式で出荷時にコンテンツ再生デバイスに記録され、メモリカードのクラス公開暗号鍵およびクラス証明書は認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａの形式で出荷時にメモリカードに記録される。また、機能証明書は、Ｃｐｂｉまたは｛Ｃｐｂｉ｝ＫＰｐｙの形式で出荷時にコンテンツ再生デバイスに記録される。後ほど詳細に説明するが、ＫＰａは配信システム全体で共通の公開認証鍵である。

【００６３】以降では、説明を簡単にするために機能証明書は、再生制御情報ＡＣｐのフラグＦＧ３～ＦＧ５によって示される地域コード、再生開始日時、再生終了日時についての対応の可否が記載され、フラグＦＧ１，ＦＧ２に対応することはコンテンツ再生デバイスにとって標準の機能であるものとする。

【００６４】また、メモリカード１１０内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵ＫＰｍｃｘと、公開暗号鍵ＫＰｍｃｘで暗号化されたデータを復号することが可能な秘密復号鍵Ｋｍｃｘとが存在する。これらのメモリカードごとに設定される公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵ＫＰｍｃｘを個別公開暗号鍵、秘密復号鍵Ｋｍｃｘを個別秘密復号鍵と称する。

【００６５】ライセンスの配信および再生が行なわれるごとに配信サーバ１０、携帯電話機１００，１０２，１０４、およびメモリカード１１０において生成される共

通鍵Ｋｓ１～Ｋｓ３が用いられる。

【００６６】ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、コンテンツ再生デバイスもしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶこととする。

【００６７】これらのセッションキーＫｓ１～Ｋｓ３は、各セッションごとに固有の値を有することにより、配信サーバ、コンテンツ再生デバイス、およびメモリカードによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキーＫｓ３は、コンテンツ再生デバイスにおいて再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行した上でライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【００６８】図５は、図１に示した配信サーバ１０の構成を示す概略ブロック図である。配信サーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータやコンテンツＩＤ等の配信情報を保持するための情報データベース３０４と、携帯電話機のユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、情報データベース３０４に保持されたコンテンツデータのメニューを保持するメニューデータベース３０７と、ライセンスの配信ごとに生成され、かつ、ライセンスを特定するライセンスＩＤ等の配信に関するログを保持する配信記録データベース３０８と、情報データベース３０４、課金データベース３０２、メニューデータベース３０７、および配信記録データベース３０８からのデータをバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【００６９】データ処理部３１０は、バスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５により制御されて、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、メモリカードから送られてきた認証のための認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを復号するための公開認証鍵ＫＰａを保持する認証鍵保持部３１３と、メモリカードから送られてきた認証のための認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを通信装置３５０およびバスＢＳ１を介して受けて、認証鍵保持部３１３からの公開認証鍵ＫＰａによって復号処理を行なう復号処理部３１２と、配信セッションごとに、セッションキー発生部３１６により生成されたセッションキーＫｓ１を復号処理部３１２によって得られたクラス公開暗号鍵ＫＰｍｗを用いて暗号化して、バスＢＳ１に出力するための暗号処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをバスＢＳ１より受けて、復号処理を行なう復号処理部３２０とを含む。

【００７０】データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンス鍵Ｋｃおよびアクセス制御情報ＡＣｍを、復号処理部３２０によって得られたメモリカードごとに個別公開暗号鍵ＫＰｍｃｘによって暗号化するための暗号処理部３２６と、暗号処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してバスＢＳ１に出力するための暗号処理部３２８とを含む。

【００７１】配信サーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００７２】図６は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

【００７３】携帯電話機１００は、携帯電話網により無線伝送される信号を受信するアンテナ１１００と、アンテナ１１００からの信号を受けてベースバンド信号に変換、あるいは携帯電話機１００からのデータを変調してアンテナ１１００に与える送受信部１１０２と、携帯電話機１００の各部のデータ授受を行なうバスＢＳ２とを含む。

【００７４】携帯電話機１００は、さらに、携帯電話機１００のユーザの音声データを取込み、音声データをＡＤ変換部１１０６へ出力するマイク１１０４と、音声データをアナログ信号からデジタル信号に変換するＡＤ変換部１１０６と、デジタル信号に変換された音声信号を所定の方式に符号化する音声符号化部１１０８とを含む。

【００７５】携帯電話機１００は、さらに、他の携帯電話機から受信した音声信号を復号する音声再生部１１１０と、音声再生部１１１０からの音声信号をデジタル信号からアナログ信号に変換して音声データを出力するＤＡ変換部１１１２と、音声データを外部へ出力するスピーカ１１１４とを含む。

【００７６】携帯電話機１００は、さらに、外部からの指示を携帯電話機１００に与える操作パネル１１１６と、コントローラ１１２０等から出力される情報をユーザに視覚情報として与える表示パネル１１１８と、バスＢＳ２を介して携帯電話機１００の動作を制御するコントローラ１１２０と、メモリカード１１０とバスＢＳ２との間のデータの授受を制御するメモリカードインタフェース１２００とを含む。

【００７７】携帯電話機１００は、さらに、クラス公開

暗号鍵ＫＰｐ１およびクラス証明書Ｃｐａ１を公開認証鍵ＫＰａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｐ１／／Ｃｐａ１｝ＫＰａを保持する認証データ保持部１５００を含む。ここで、携帯電話機１００のクラスｙは、ｙ＝１であるとする。

【００７８】携帯電話機１００は、さらに、クラス固有の復号鍵であるＫｐ１を保持するＫｐ保持部１５０２と、バスＢＳ２から受けたデータをＫｐ１によって復号し、メモリカード１１０によって発生されたセッションキーＫｓ２を得る復号処理部１５０４とを含む。

【００７９】携帯電話機１００は、さらに、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセッションキー発生部１５０８と、機能証明書Ｃｐｂｉを保持する機能証明書保持部１５０７とを含む。ここで、携帯電話機１００のクラスｉは、ｉ＝１であるとする。機能証明書Ｃｐｂ１は、コンテンツ再生デバイス１５５０が時間を判定する機能を備えることを示す機能証明書である。

【００８０】携帯電話機１００は、さらに、暗号化コンテンツデータの再生セッションにおいてメモリカード１１０からライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを受取る際に、機能証明書保持部１５０７からの機能証明書Ｃｐｂ１とセッションキー発生部１５０８により発生されたセッションキーＫｓ３とを復号処理部１５０４によって得られたセッションキーＫｓ２によって暗号化し、バスＢＳ２に出力する暗号処理部１５０６と、バスＢＳ２上のデータをセッションキーＫｓ３によって復号して、ライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを出力する復号処理部１５１０と、時間情報を出力する時計１５１２と、復号処理部１５１０からライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを受け、その受けた再生制御情報ＡＣｐに含まれる再生開始日時または再生終了日時と時計１５１２から得られた時間情報とに基づいて暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの再生が時期的に制限されているか否かを判定し、再生が時期的に制限されていないとき、ライセンス鍵Ｋｃを復号処理部１５１６へ出力する再生制御部１５１４とを含む。

【００８１】携帯電話機１００は、さらに、バスＢＳ２より暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを受けて、再生制御部１５１４からのライセンス鍵Ｋｃによって暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号してコンテンツデータＤｃを音楽再生部１５１８へ出力する復号処理部１５１６と、復号処理部１５１６からの出力を受けてコンテンツデータを再生するための音楽再生部１５１８と、音楽再生部１５１８の出力をディジタル信号からアナログ信号に変換するＤＡ変換部１５１９と、ＤＡ変換部１５１９の出力をヘッドホーンなどの外部出力装置（図示省略）へ出力するための端子１５３０とを含む。

【００８２】なお、図６においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生デバイス１５５０を構成する。

【００８３】このように、携帯電話機１００は、再生制御情報ＡＣｐによって制限される暗号化コンテンツデータの再生期間を判定する機能を備える携帯電話機である。

【００８４】図７は、図１に示すデータ配信システムにおける携帯電話機１０２の構成を説明するための概略ブロック図である。携帯電話機１０２は、携帯電話機１００の時計１５１２を削除したものであり、その他は携帯電話機１００と同じである。なお、携帯電話機１０２においては、機能証明書保持部１５０７は、機能証明書Ｃｐｂ１に代えて機能証明書Ｃｐｂ２を保持する。機能証明書Ｃｐｂ２は、コンテンツ再生デバイス１５５０が時間的な判定機能を有しないことを示す機能証明書である。したがって、携帯電話機１０２は、再生制御情報ＡＣｐによって制限される暗号化コンテンツデータの再生期間を判定できない携帯電話機である。

【００８５】図８は、図１に示すデータ配信システムにおける携帯電話機１０４の構成を説明するための概略ブロック図である。携帯電話機１０４は、携帯電話機１００の機能証明書保持部１５０７および時計１５１２を削除したものであり、その他は携帯電話機１００と同じである。したがって、携帯電話機１０４は、機能証明書を備えない携帯電話機である。

【００８６】携帯電話機１００，１０２，１０４の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００８７】図９は、図１に示すメモリカード１１０の構成を説明するための概略ブロック図である。

【００８８】すでに説明したように、メモリカードのクラス公開暗号鍵およびクラス秘密復号鍵として、ＫＰｍｗおよびＫｍｗが設けられ、メモリカードのクラス証明書Ｃｍｗが設けられるが、メモリカード１１０においては、自然数ｗ＝３で表わされるものとする。また、メモリカードを識別する自然数ｘはｘ＝４で表されるものとする。

【００８９】したがって、メモリカード１１０は、認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを保持する認証データ保持部１４００と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵Ｋｍｃ４を保持するＫｍｃ保持部１４０２と、クラス秘密復号鍵Ｋｍ３を保持するＫｍ保持部１４２１と、個別秘密復号鍵Ｋｍｃ４によって復号可能な公開暗号鍵ＫＰｍｃ４を保持するＫＰｍｃ保持部１４１６とを含む。

【００９０】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかに

なるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【００９１】メモリカード１１０は、さらに、メモリインタフェース１２００との間で信号を端子１４２６を介して授受するインタフェース１４２４と、インタフェース１４２４との間で信号をやり取りするバスＢＳ３と、バスＢＳ３にインタフェース１４２４から与えられるデータから、クラス秘密復号鍵Ｋｍ３をＫｍ保持部１４２１から受けて、配信サーバ１０が配信セッションにおいて生成したセッションキーＫｓ１を接点Ｐａに出力する復号処理部１４２２と、ＫＰａ保持部１４１４から公開認証鍵ＫＰａを受けて、バスＢＳ３に与えられるデータから公開認証鍵ＫＰａによる復号処理を実行して復号結果と得られたクラス証明書をコントローラ１４２０に、得られたクラス公開鍵を暗号化処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４６によって選択的に与えられるデータを暗号化してバスＢＳ３に出力する暗号処理部１４０６とを含む。

【００９２】メモリカード１１０は、さらに、配信、および再生の各セッションにおいてセッションキーＫｓ２を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ２を復号処理部１４０８によって得られるクラス公開暗号鍵ＫＰｐｙによって暗号化してバスＢＳ３に送出する暗号処理部１４１０と、バスＢＳ３よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ２によって復号する復号処理部１４１２とを含む。

【００９３】メモリカード１１０は、さらに、バスＢＳ３上のデータを個別公開暗号鍵ＫＰｍｃ４と対をなすメモリカード１１０の個別秘密復号鍵Ｋｍｃ４によって復号するための復号処理部１４０４と、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを再生するためのライセンス（Ｋｃ，ＡＣｐ，ＡＣｍ，ライセンスＩＤ，コンテンツＩＤ）と、付加情報Ｄｃ－ｉｎｆと、暗号化コンテンツデータの再生リストと、ライセンスを管理するためのライセンス管理ファイルとをバスＢＳ３より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。また、メモリ１４１５は、ライセンス領域１４１５Ａと、データ領域１４１５Ｂとから成る。

【００９４】ライセンス領域１４１５Ａは、ライセンスを記録するための領域であり、ライセンス（ライセンス鍵Ｋｃ、再生制御情報ＡＣｐ、アクセス制限情報ＡＣｍ、ライセンスＩＤ、コンテンツＩＤ）を記録するためにエントリと呼ばれるライセンス専用の記録単位でライセンスを格納する。ライセンスに対してアクセスする場合には、ライセンスが格納されている、あるいは、ライセンスを記録したいエントリをエントリ番号によって指定する構成になっている。

【００９５】データ領域１４１５Ｂは、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ、暗号化コンテンツデータの関連情報Ｄｃ－ｉｎｆ、ライセンスを管理するために必要な情報を暗号化コンテンツデータごとに記録するライセンス管理ファイル、メモリカードに記録された暗号化コンテンツデータやライセンスにアクセスするための基本的な情報を記録する再生リスト、およびライセンス領域１４１５Ａのエントリを管理するためのエントリ情報を記録するための領域である。そして、データ領域１４１５Ｂは、外部から直接アクセスが可能である。ライセンス管理ファイルおよび再生リストの詳細については後述する。

【００９６】メモリカード１１０は、さらに、バスＢＳ３を介して外部との間でデータ授受を行ない、バスＢＳ３との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０を含む。

【００９７】なお、データ領域１４１５Ｂを除く全ての構成は、耐タンパモジュール領域に構成される。

【００９８】以下、図１に示すデータ配信システムにおける各セッションの動作について説明する。

【００９９】［配信］まず、図１に示すデータ配信システムにおいて、配信サーバ１０から携帯電話機１００，１０２，１０４に装着されたメモリカード１１０へ暗号化コンテンツデータおよびライセンスを配信する動作について説明する。

【０１００】図１０および図１１は、図１に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生する携帯電話機１００，１０２，１０４に装着されたメモリカード１１０へのライセンスの配信動作（以下、配信セッションともいう）を説明するための第１および第２のフローチャートである。

【０１０１】図１０における処理以前に、携帯電話機１００，１０２，１０４のユーザは、配信サーバ１０に対して電話網を介して接続し、購入を希望するコンテンツに対するコンテンツＩＤを取得し、さらに、メモリカード１１０に対するエントリ管理情報を取得してライセンス領域１４１５Ａ内の空きエントリを確認していることを前提としている。

【０１０２】図１０を参照して、携帯電話機１００，１０２，１０４のユーザから操作パネル１１１６を介してコンテンツＩＤの指定による配信リクエストがなされる（ステップＳ１００）。そして、操作パネル１１１６を介して暗号化コンテンツデータのライセンスを購入するための購入条件ＡＣを入力するように指示し、購入条件ＡＣが入力される（ステップＳ１０２）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Ｋｃを購入するために、暗号化コンテンツデータのアクセ

ス制御情報ＡＣｍ、および再生制御情報ＡＣｐを設定して購入条件ＡＣが入力される。

【０１０３】暗号化コンテンツデータの購入条件ＡＣが入力されると、コントローラ１１２０は、バスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１０へ認証データの出力指示を与える（ステップＳ１０４）。メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介して認証データの送信要求を受信する（ステップＳ１０６）。そして、コントローラ１４２０は、バスＢＳ３を介して認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを読出し、｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ３、インタフェース１４２４および端子１４２６を介して出力する（ステップＳ１０８）。

【０１０４】携帯電話機１００，１０２，１０４のコントローラ１１２０は、メモリカード１１０からの認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａに加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣ；および配信リクエストを配信サーバ１０に対して送信する（ステップＳ１１０）。

【０１０５】配信サーバ１０では、携帯電話機１００，１０２，１０４から配信リクエスト、コンテンツＩＤ、認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ、およびライセンス購入条件のデータＡＣを受信し（ステップＳ１１２）、復号処理部３１２においてメモリカード１１０から出力された認証データを公開認証鍵ＫＰａで復号する（ステップＳ１１４）。

【０１０６】配信制御部３１５は、復号処理部３１２における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１６）。正当な認証データであると判断された場合、配信制御部３１５は、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ１１８）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで配信セッションを終了する（ステップＳ１６４）。

【０１０７】認証の結果、正当な認証データを持つメモリカードを装着した携帯電話機からのアクセスであることが確認されると、配信サーバ１０において、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する（ステップＳ１１８）。セッションキーＫｓ１は、復号処理部３１２によって得られたメモリカード１１０に対応するクラス公開暗号鍵ＫＰｍ３によって、暗号処理部３１８によって暗号化される（ステップＳ１２０）。

【０１０８】配信制御部３１５は、ライセンスＩＤを生成し（ステップＳ１２２）、ライセンスＩＤおよび暗号化されたセッションキーＫｓ１は、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ３として、バスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１２４）。

【０１０９】携帯電話機１００，１０２，１０４が、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ３を受信すると、コントローラ１１２０は、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ３をメモリカード１１０に入力する（ステップＳ１２６）。そうすると、メモリカード１１０においては、端子１４２６およびインタフェース１４２４を介して、コントローラ１４２０は、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ３を受理する（ステップＳ１２８）。そして、コントローラ１４２０は、バスＢＳ３を介して｛Ｋｓ１｝Ｋｍ３を復号処理部１４２２へ与え、復号処理部１４２２は、Ｋｍ保持部１４２１に保持されるメモリカード１１０に固有なクラス秘密復号鍵Ｋｍ３によって復号処理することにより、セッションキーＫｓ１を復号し、セッションキーＫｓ１を受理する（ステップＳ１３２）。

【０１１０】コントローラ１４２０は、配信サーバ１０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部１４１８に対してメモリカード１１０において配信動作時に生成されるセッションキーＫｓ２の生成を指示する。そして、セッションキー発生部１４１８は、セッションキーＫｓ２を生成する（ステップＳ１３４）。

【０１１１】暗号処理部１４０６は、切換スイッチ１４４２の接点Ｐａを介して復号処理部１４２２より与えられるセッションキーＫｓ１によって、切換スイッチ１４４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、および個別公開暗号鍵ＫＰｍｃ４を１つのデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍｃ４｝Ｋｓ１をバスＢＳ３に出力する。バスＢＳ３に出力された暗号化データ｛Ｋｓ２／／ＫＰｍｃ４｝Ｋｓ１は、バスＢＳ３からインタフェース１４２４および端子１４２６を介して携帯電話機１００，１０２，１０４に出力され（ステップＳ１３８）、携帯電話機１００，１０２，１０４から配信サーバ１０に送信される（ステップＳ１４０）。

【０１１２】図１１を参照して、配信サーバ１０は、｛Ｋｓ２／／ＫＰｍｃ４｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、メモリカード１１０で生成されたセッションキーＫｓ２、およびメモリカード１１０の個別公開暗号鍵ＫＰｍｃ４を受理する（ステップＳ１４２）。

【０１１３】配信制御部３１５は、ステップＳ１１２で取得したコンテンツＩＤに従ってライセンス鍵Ｋｃを情報データベース３０４から取得し（ステップＳ１４４）、ステップＳ１１２で取得したライセンス購入条件のデータＡＣに従って、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐを決定する（ステップＳ１４６）。

【０１１４】配信制御部３１５は、生成したライセン

ス、すなわち、ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、再生制御情報ＡＣｐ、およびアクセス制御情報ＡＣｍを暗号処理部３２６に与える。暗号処理部３２６は、復号処理部３２０によって得られたメモリカード１１０の個別公開暗号鍵ＫＰｍｃ４によってライセンスを暗号化して暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を生成する（ステップＳ１４８）。そして、暗号処理部３２８は、暗号処理部３２６からの暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を、復号処理部３２０からのセッションキーＫｓ２によって暗号化し、暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を出力する。配信制御部３１５は、バスＢＳ１および通信装置３５０を介して暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を携帯電話機１００，１０２，１０４へ送信する（ステップＳ１５０）。

【０１１５】携帯電話機１００，１０２，１０４は、送信された暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信し、バスＢＳ２を介してメモリカード１１０に入力する（ステップＳ１５２）。メモリカード１１０においては、端子１４２６およびインタフェース１４２４を介して、バスＢＳ３に与えられた受信データを復号処理部１４１２によって復号する。復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２を用いてバスＢＳ３の受信データを復号し、バスＢＳ３に出力する（ステップＳ１５４）。

【０１１６】この段階で、バスＢＳ３には、Ｋｍｃ保持部１４０２に保持される個別秘密復号鍵Ｋｍｃ４で復号可能な暗号化ライセンス｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４が出力される（ステップＳ１５４）。

【０１１７】コントローラ１４２０の指示によって、暗号化ライセンス｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４は、復号処理部１４０４において、個別秘密復号鍵Ｋｍｃ４によって復号され、ライセンス（ライセンス鍵Ｋｃ、ライセンスＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）が受理される（ステップＳ１５６）。

【０１１８】携帯電話機１００，１０２，１０４のコントローラ１１２０は、メモリカード１１０のメモリ１４１５から読出したエントリ管理情報に基づいて、配信サーバ１０から受信したライセンスを格納するためのエントリ番号を決定し、その決定したエントリ番号をバスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１０へ入力する。そして、コントローラ１１２０は、エントリ管理情報を追加更新する（ステップＳ１５８）。

【０１１９】そうすると、メモリカード１１０のコントローラ１４２０は、端子１４２６およびインタフェース１４２４を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ１４１５のライセンス領域１４１５Ａに、ステップＳ１５６において取得したライセンス（ライセンス鍵Ｋｃ、ライセンスＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）を格納する（ステップＳ１６０）。ライセンスの書込みが終了すると、コントローラ１１２０は、ステップＳ１５８においてメモリカード１１０へ入力したエントリが使用中であるようにエントリ管理情報を更新し、その更新したエントリ管理情報をメモリカード１１０へ入力する（ステップＳ１６２）。メモリカード１１０のコントローラ１４２０は、入力されたエントリ管理情報を用いてメモリ１４１５のデータ領域１４１５Ｂ内にエントリ管理情報を書込む（ステップＳ１６３）。そして、ライセンスの配信動作が終了する（ステップＳ１６４）。

【０１２０】ライセンスの配信セッションが終了した後、携帯電話機１００，１０２，１０４のコントローラ１１２０は、暗号化コンテンツデータの配信要求を配信サーバ１０へ送信し、配信サーバ１０は、暗号化コンテンツデータの配信要求を受信する。そして、配信サーバ１０の配信制御部３１５は、情報データベース３０４より、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して出力する。

【０１２１】携帯電話機１００，１０２，１０４は、｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信して、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを受理する。そうすると、コントローラ１１２０は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを１つのコンテンツファイルとしてバスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１０に入力する。また、コントローラ１１２０は、メモリカード１１０に格納されたライセンスのエントリ番号と、平文のライセンスＩＤおよびコンテンツＩＤを含む暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆに対するライセンス管理ファイルを生成し、バスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１０に入力する。さらに、コントローラ１１２０は、メモリカード１１０のメモリ１４１５に記録されている再生リストに、受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や付加情報Ｄｃ－ｉｎｆから抽出した暗号化コンテンツデータに関する情報（曲名、アーティスト名）等を追記し、全体の処理が終了する。

【０１２２】このようにして、携帯電話機１００，１０２，１０４に装着されたメモリカード１１０が正規の認証データを保持する機器であること、同時に、クラス証明書Ｃｍ３とともに暗号化して送信できた公開暗号鍵ＫＰｍ３が有効であることを確認した上でコンテンツデータを配信することができ、不正なメモリカードへのコンテンツデータの配信を禁止することができる。

【０１２３】さらに、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【０１２４】図１２を参照して、メモリカード１１０のメモリ１４１５におけるライセンス領域１４１５Ａとデータ領域１４１５Ｂとについて説明する。データ領域１４１５Ｂには、再生リストファイル１６０と、エントリ管理情報１６５と、コンテンツファイル１６１１～１６１ｎと、ライセンス管理ファイル１６２１～１６２ｎとが記録されている。コンテンツファイル１６１１～１６１ｎは、受信した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとを１つのファイルとして記録する。また、ライセンス管理ファイル１６２１～１６２ｎは、それぞれ、コンテンツファイル１６１１～１６１ｎに対応して記録されている。

【０１２５】メモリカード１１０は、配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信したとき、暗号化コンテンツデータおよびライセンスをメモリ１４１５に記録する。

【０１２６】したがって、配信サーバ１０からメモリカード１１０へ送信された暗号化コンテンツデータのライセンスは、メモリ１４１５のライセンス領域１４１５Ａのエントリ番号によって指定された領域に記録され、メモリ１４１５のデータ領域１４１５Ｂに記録された再生リストファイル１６０のライセンス管理ファイルを読出せば、エントリ番号を取得でき、その取得したエントリ番号によって対応するライセンスをライセンス領域１４１５Ａから読出すことができる。

【０１２７】［再生］上述したように、携帯電話機１００，１０２，１０４に装着されたメモリカード１１０は、配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信できる。そこで、次に、メモリカードが受信した暗号化コンテンツデータの再生について説明する。

【０１２８】図１３は、メモリカード１１０が受信したコンテンツデータの携帯電話機１００，１０２，１０４における再生動作を説明するためのフローチャートである。なお、図１３における処理以前に、携帯電話機１００，１０２，１０４のユーザは、メモリカード１１０のデータ領域１４１５Ｂに記録されている再生リストに従って、再生するコンテンツ（楽曲）を決定し、コンテンツファイルを特定し、ライセンス管理ファイルを取得していることを前提として説明する。

【０１２９】図１３を参照して、再生動作の開始とともに、携帯電話機１００，１０２，１０４のユーザから操作パネル１１１６を介して再生リクエストが携帯電話機１００，１０２，１０４にインプットされる（ステップＳ１０）。そうすると、携帯電話機１００，１０２，１０４とメモリカード１１０との間で初期化処理が行なわれる（ステップＳ２０）。この初期化処理の詳細については後述する。初期化処理が終了すると、携帯電話機１００，１０２，１０４のコントローラ１１２０は、初期化処理においてエラーが発生したか否かを判定し（ステップＳ３０）、エラーが発生した場合は、暗号化コンテンツデータの再生動作は終了する（ステップＳ７０）。

【０１３０】ステップＳ３０において、コントローラ１１２０が初期化処理においてエラーが発生していないと判定したとき、再生許諾処理が行なわれる（ステップＳ４０）。この再生許諾処理の詳細についても後述する。再生許諾処理が終了すると、携帯電話機１００，１０２，１０４のコントローラ１１２０は、再生許諾処理においてエラーが発生したか否かを判定し（ステップＳ５０）、エラーが発生したとき再生許諾処理（ステップＳ４０）を繰返し行なう。ステップＳ５０において、コントローラ１１２０が再生許諾処理においてエラーが発生しなかったと判定したとき、再生処理が行なわれる（ステップＳ６０）。その後、ステップＳ４０，Ｓ５０，Ｓ６０が繰返されて暗号化コンテンツデータの再生が行なわれる。したがって、再生動作において、一度、初期化処理を行なえば、２回目以降、初期化処理を行なうことなく、暗号化コンテンツデータを再生することができる。

【０１３１】図１４は、図１３に示す初期化処理の動作を詳細に説明するためのフローチャートである。図１４を参照して、図１３に示すステップＳ１０において再生リクエストがされると、コントローラ１１２０は、バスＢＳ２を介して認証データの出力要求をコンテンツ再生デバイス１５５０に行ない（ステップＳ２００）、コンテンツ再生デバイス１５５０は認証データの出力要求を受信する（ステップＳ２０２）。そして、認証データ保持部１５００は、認証データ｛ＫＰｐ１／／Ｃｐａ１｝ＫＰａを出力し（ステップＳ２０４）、コントローラ１１２０は、メモリカードインタフェース１２００を介してメモリカード１１０へ認証データ｛ＫＰｐ１／／Ｃｐａ１｝ＫＰａを入力する（ステップＳ２０６）。

【０１３２】そうすると、メモリカード１１０は、認証データ｛ＫＰｐ１／／Ｃｐａ１｝ＫＰａを受理し（ステップＳ２０８）、復号処理部１４０８は、受理した認証データ｛ＫＰｐ１／／Ｃｐａ１｝ＫＰａを、ＫＰａ保持

部１４１４に保持された公開認証鍵ＫＰａによって復号し（ステップＳ２１０）、コントローラ１４２０は復号処理部１４０８における復号処理結果から、認証処理を行なう。すなわち、認証データ｛ＫＰｐｌ／／Ｃｐａ１｝ＫＰａが正規の認証データであるか否かを判断する認証処理を行なう（ステップＳ２１２）。復号できなかった場合、ステップＳ２２２へ移行し、初期化処理は終了する。認証データが復号できた場合、コントローラ１４２０は、セッションキー発生部１４１８を制御し、セッションキー発生部１４１８は、再生セッション用のセッションキーＫｓ２を発生させる（ステップＳ２１４）。そして、暗号処理部１４１０は、セッションキー発生部１４１８からのセッションキーＫｓ２を、復号処理部１４０８で復号された公開暗号鍵ＫＰｐ１によって暗号化した暗号化データ｛Ｋｓ２｝Ｋｐ１をバスＢＳ３へ出力する。そうすると、コントローラ１４２０は、インタフェース１４２４および端子１４２６を介してメモリカードインタフェース１２００へ暗号化データ｛Ｋｓ２｝Ｋｐ１を出力する（ステップＳ２１６）。携帯電話機１００，１０２，１０４のコントローラ１１２０は、メモリカードインタフェース１２００を介して暗号化データ｛Ｋｓ２｝Ｋｐ１を取得する。そして、コントローラ１１２０は、暗号化データ｛Ｋｓ２｝Ｋｐ１をバスＢＳ２を介してコンテンツ再生デバイス１５５０の復号処理部１５０４へ与え（ステップＳ２１８）、復号処理部１５０４は、Ｋｐ保持部１５０２から出力された、公開暗号鍵ＫＰｐ１と対になっている秘密復号鍵Ｋｐ１によって暗号化データ｛Ｋｓ２｝Ｋｐ１を復号し、セッションキーＫｓ２を受理する（ステップＳ２２０）。そして、初期化処理が終了する（ステップＳ２２２）。

【０１３３】図１５は、図１３に示す再生許諾処理（ステップＳ４０）の動作を詳細に説明するためのフローチャートである。なお、図１５は、携帯電話機１００，１０２とメモリカード１１０との間における再生許諾処理の動作を示したフローチャートである。図１５を参照して、図１３に示すステップＳ３０においてエラーが発生しなかったと判定されると、携帯電話機１００，１０２のコントローラ１１２０は、セッションキーＫｓ３を発生するようにセッションキー発生部１５０８を制御し（ステップＳ３００）、セッションキー発生部１５０８は、再生セッション用のセッションキーＫｓ３を発生させ、セッションキーＫｓ３を暗号処理部１５０６へ出力する（ステップＳ３０４）。暗号処理部１５０６は、セッションキー発生部１５０８からのセッションキーＫｓ３と機能証明書保持部１５０７からの機能証明書Ｃｐｂｉとを復号処理部１５０４からのセッションキーＫｓ２によって暗号化して｛Ｋｓ３／／Ｃｐｂｉ｝Ｋｓ２を出力し（ステップＳ３０６）、コントローラ１１２０は、バスＢＳ２およびメモリカードインタフェース１２００を介して｛Ｋｓ３／／Ｃｐｂｉ｝Ｋｓ２をメモリカード１１０へ出力する（ステップＳ３０８）。

【０１３４】そうすると、メモリカード１１０の復号処理部１４１２は、端子１４２６、インタフェース１４２４、およびバスＢＳ３を介して｛Ｋｓ３／／Ｃｐｂｉ｝Ｋｓ２を受ける。復号処理部１４１２は、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって｛Ｋｓ３／／Ｃｐｂｉ｝Ｋｓ２を復号して、携帯電話機１００，１０２で発生されたセッションキーＫｓ３と機能証明書Ｃｐｂｉとを受理する（ステップＳ３１０）。

【０１３５】携帯電話機１００，１０２のコントローラ１１２０は、メモリカード１１０から事前に取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し、取得したエントリ番号とライセンス出力要求とをメモリカードインタフェース１２００を介してメモリカード１１０へ入力する（ステップＳ３１２）。

【０１３６】メモリカード１１０のコントローラ１４２０は、エントリ番号とライセンス出力要求とを受理し、エントリ番号によって指定された領域に格納されたライセンスを取得する（ステップＳ３１４）。そして、コントローラ１４２０は、取得したライセンスから再生制御情報ＡＣｐを読出して再生制御情報ＡＣｐ内の再生制限フラグを確認し、ステップＳ３１４において受理した機能証明書Ｃｐｂｉによって再生制限フラグがアクティブ「１」となっている再生制限に従って再生を行なう機能を備えているか否か、すなわち、機能証明書を出力したコンテンツ再生デバイス１５５０が再生制御情報ＡＣｐに対応しているか否かを判定する（ステップＳ３１６）。

【０１３７】メモリカード１１０が携帯電話機１００から機能証明書を受理したとき、その機能証明書は、携帯電話機１００のコンテンツ再生デバイス１５５０が時間を判定する機能を備えていることを示す機能証明書Ｃｐｂ１であるので、コントローラ１４２０は、再生制御情報ＡＣｐの時間に関する制限があることを示すフラグＦＧ４，ＦＧ５のいずれかがアクティブ「１」の場合には対応できると判断する。フラグＦＧ４，ＦＧ５が共にネガティブ「０」の場合には、時間に関する制限を受けないため、コントローラ１４２０は、対応できると判断する。

【０１３８】一方、メモリカード１１０が携帯電話機１０２から機能証明書を受理したとき、その機能証明書は、携帯電話機１０２のコンテンツ再生デバイス１５５０が時間を判定する機能を備えないことを示す機能証明書Ｃｐｂ２であるので、コントローラ１４２０は、再生制御情報ＡＣｐの時間に関する制限があることを示すフラグＦＧ４，ＦＧ５のいずれかがアクティブ「１」の場合には対応できないと判断する。フラグＦＧ４，ＦＧ５が共にネガティブ「０」の場合には、時間に関する制限

を受けないため、コントローラ１４２０は、対応できると判断する。また、コントローラ１４２０は、再生制御情報ＡＣｐにおいて再生開始日時および再生終了日時の指定がなされていないとき、機能証明書Ｃｐｂ２が再生制御情報ＡＣｐに対応していると判定する。

【０１３９】また、フラグＦＧ３については、携帯電話機１００または携帯電話機１０２のコンテンツ再生デバイス１５５０が地域コードを保持し、その地域コードに対応した地域で再生を許可されたコンテンツデータのみを再生する場合、それぞれの機能証明書には、地域コード対応が記載されていることとなり、フラグＦＧ３がアクティブ「１」の場合には、機能証明書によって地域コード対応とされた場合に対応可能と判断する。逆に、フラグＦＧ３がネガティブ「０」の場合には、地域コードによる制限を受けない全地域において再生が可能なコンテンツであり、機能証明書によらないで全ての機器において対応可能と判断する。他のフラグＦＧ１，ＦＧ２についても同様である。

【０１４０】このようにしてステップＳ３１６では、再生制限フラグを構成する全てのフラグＦＧ１～ＦＧ５に対して対応可能であると判断されたとき、コントローラ１４２０は、再生制御情報ＡＣｐに記載されていると判断し、いずれか一つでも対応できない場合には対応不可と判断する。

【０１４１】ステップＳ３１６において、コントローラ１４２０は、機能証明書Ｃｐｂｉによってコンテンツ再生デバイス１５５０が再生制御情報ＡＣｐに対応していないと判定したとき、再生許諾処理は終了する（ステップＳ３３０）。ステップＳ３１６において、コントローラ１４２０は、機能証明書Ｃｐｂｉが再生制御情報ＡＣｐに対応していると判定したとき、ライセンスに含まれるアクセス制限情報ＡＣｍを確認する（ステップＳ３１８）。

【０１４２】ステップＳ３１８においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣｍを確認することにより、具体的には、再生回数を確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に制限がある場合にはアクセス制限情報ＡＣｍの再生回数を変更した（ステップＳ３２０）後に次のステップに進む（ステップＳ３２２）。一方、アクセス制限情報ＡＣｍの再生回数によって再生が制限されていない場合においては、ステップＳ３１８はスキップされ、アクセス制限情報ＡＣｍの再生回数は変更されることなく処理が次のステップ（ステップＳ３２２）に進行される。

【０１４３】ステップＳ３１８において、当該再生動作において再生が可能であると判断された場合には、メモリ１４１５のライセンス領域１４１５Ａに記録された再生リクエスト曲のライセンス鍵Ｋｃおよび再生制御情報ＡＣｐがバスＢＳ３上に出力される（ステップＳ３２２）。

【０１４４】得られたライセンス鍵Ｋｃと再生制御情報ＡＣｐは、バスＢＳ３を介して暗号処理部１４０６に送られる。暗号処理部１４０６は、切換スイッチ１４４２の接点Ｐｂを介して復号処理部１４１２より受けたセッションキーＫｓ３によってバスＢＳ３を介して受けたライセンス鍵Ｋｃと再生制御情報ＡＣｐとを暗号化し、｛Ｋｃ／／ＡＣｐ｝Ｋｓ３をバスＢＳ３に出力する。

【０１４５】バスＢＳ３に出力された暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３は、インタフェース１４２４、端子１４２６、およびメモリカードインタフェース１２００を介して携帯電話機１００，１０２に出力される（ステップＳ３２２）。

【０１４６】携帯電話機１００，１０２のコントローラ１１２０は、メモリカードインタフェース１２００およびバスＢＳ２を介して暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３を受取り、その受取った暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３をバスＢＳ２を介してコンテンツ再生デバイス１５５０の復号処理部１５１０に与える（ステップＳ３２４）。そして、復号処理部１５１０は、バスＢＳ２を介して与えられた暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３を、セッションキー発生部１５０８からのセッションキーＫｓ３によって復号処理を行ない、ライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを再生制御部１５１４へ出力する。これによってライセンス鍵Ｋｃおよび再生制御情報ＡＣｐが受理される（ステップＳ３２６）。

【０１４７】再生制御部１５１４は、再生制御情報ＡＣｐに基づいて暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの再生が可能か否かを判定する（ステップＳ３２８）。具体的には、携帯電話機１００の場合、コンテンツ再生デバイスはフラグＦＧ３～ＦＧ５に対応しているとすると、再生制御部１５１４は、再生制限フラグのフラグＦＧ３～ＦＧ５のいずれがアクティブ「１」であるかを確認する。そして、フラグＦＧ３がアクティブ「１」である場合、再生制御部１５１４は、内部に保持した地域コードを、再生制御情報ＡＣｐの領域２１に記載されている地域コードと比較し、不一致であるとき再生許諾動作を終了する。また、フラグＦＧ４またはフラグＦＧ５がアクティブ「１」である場合、再生制御部１５１４は、時計１５１２から時間情報を取得し、その取得した時間情報と再生制御情報ＡＣｐに含まれる再生開始日時または再生終了日時とに基づいて、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの再生が再生開始日時または再生終了日時によって制限されているか否かを判定し、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの再生が再生開始日時または再生終了日時によって制限されているとき、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの再生許諾動作が終了する（ステップＳ３３０）。再生制御部１５１４は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの再生が再生制御情報ＡＣｐによ

って制限されていないと判定したとき、ライセンス鍵Ｋｃを復号処理部１５１６へ出力し、後述する暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの再生処理が行なわれる。

【０１４８】一方、携帯電話機１０２の場合、コンテンツ再生デバイスは、フラグＦＧ３にのみ対応し、フラグＦＧ４，ＦＧ５には対応しない。しかし、ステップＳ３１６の処理によってフラグＦＧ４，ＦＧ５は必ずネガティブ「０」である。再生制御部１５１４は、再生制限フラグのフラグがアクティブ「１」であるかを確認する。そして、フラグＦＧ３がアクティブ「１」である場合、再生制御部１５１４は、内部に保持した地域コードを、再生制御情報ＡＣｐの領域２１に記載されている地域コードと比較して不一致のとき再生許諾動作が終了する（ステップＳ３３０）。再生制御部１５１４は、保持した地域コードが再生制御情報ＡＣｐの領域２１に記載された地域コードと一致したとき、ライセンス鍵Ｋｃを復号処理部１５１６へ出力し、後述する暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの再生処理が行なわれる。

【０１４９】そして、再生許諾処理が終了する（ステップＳ３３０）。このように、再生許諾処理においては、携帯電話機１００，１０２からメモリカード１１０へ送信された機能証明書Ｃｐｂｉが暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの再生制御情報ＡＣｐに対応しているか否かがメモリカード１１０において判定され（ステップＳ３１６参照）、機能証明書Ｃｐｂｉが再生制御情報ＡＣｐに対応していないとき再生許諾処理が終了する。したがって、再生制御情報ＡＣｐによって制限される機能に対応する機能を備えない携帯電話機にメモリカードが装着されたとき、暗号化コンテンツデータを復号および再生するためのライセンスはメモリカード１１０から携帯電話機１００，１０２へ出力されず、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの再生を制限することができる。

【０１５０】再生許諾処理のステップＳ３２８において、再生制御部１５１４は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの再生が可能であると判定したとき、その判定結果をバスＢＳ２を介してコントローラ１１２０へ出力し、ライセンス鍵Ｋｃを復号処理部１５１６へ出力する。そして、コントローラ１１２０は、メモリカードインタフェース１２００を介してメモリカード１１０に暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを要求する。そうすると、メモリカード１１０のコントローラ１４２０は、メモリ１４１５から暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、バスＢＳ３、インタフェース１４２４、および端子１４２６を介してメモリカードインタフェース１２００へ暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを出力する。

【０１５１】携帯電話機１１０，１０２のコントローラ１１２０は、メモリカードインタフェース１２００を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、バスＢＳ２を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃをコンテンツ再生デバイス１５５０へ与える。

【０１５２】そして、コンテンツ再生デバイス１５５０の復号処理部１５１６は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを再生制御部１５１４から出力されたライセンス鍵Ｋｃによって復号してコンテンツデータＤｃを取得する。

【０１５３】そして、復号されたコンテンツデータＤｃは音楽再生部１５１８へ出力され、音楽再生部１５１８は、コンテンツデータＤｃを再生し、ＤＡ変換部１５１９はディジタル信号をアナログ信号に変換して端子１５３０へ出力する。そして、音楽データは端子１５３０から外部出力装置を介してヘッドホーン１３０へ出力されて再生される。これによって再生動作が終了する。

【０１５４】また、機能証明書を備えない携帯電話機１０４における再生許諾処理は、図１５のステップＳ３０６，Ｓ３０８，Ｓ３１０を図１６に示すステップＳ３０６ａ，Ｓ３０８ａ，Ｓ３１０ａ，Ｓ３１１に代えたフローチャートに従って行なわれる。図１５に示すステップＳ３０４の後、携帯電話機１０４の暗号処理部１５０６は、セッションキー発生部１５０８からのセッションキーＫｓ３を、復号処理部１５０４からのセッションキーＫｓ２によって暗号化して暗号化データ｛Ｋｓ３｝Ｋｓ２をバスＢＳ２へ出力する（ステップＳ３０６ａ）。そして、コントローラ１１２０は、暗号化データ｛Ｋｓ３｝Ｋｓ２をバスＢＳ２を介して受理し、メモリカードインタフェース１２００を介してメモリカード１１０へ出力する（ステップＳ３０８ａ）。そうすると、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ３を介して暗号化データ｛Ｋｓ３｝Ｋｓ２を受取り、その受取った暗号化データ｛Ｋｓ３｝Ｋｓ２をバスＢＳ３を介して復号処理部１４１２に与える。復号処理部１４１２は、暗号化データ｛Ｋｓ３｝Ｋｓ２を、セッションキー発生部１４１８からのセッションキーＫｓ２によって復号する（ステップＳ３１０ａ）。

【０１５５】そうすると、コントローラ１４２０は、ステップＳ３１０ａにおいて機能証明書が入力されてこないのでコンテンツ再生デバイスに要求される標準の機能が備えられているものとして、デフォルト値を携帯電話機１０４に内蔵されたコンテンツ再生デバイス１５５０の機能証明書Ｃｐｂｉとして受理する（ステップＳ３１１）。ステップＳ３１１の後、図１５に示すステップＳ３１２～Ｓ３３０が実行されて携帯電話機１０４における再生許諾処理が終了する。ステップＳ３１１において受理されたデフォルト値は、図３に示すフラグＦＧ１，ＦＧ２による再生制限に対応可能であり、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの再生制御情報ＡＣｐに再生速度および編集可否に関する制限情報が設定されている場合は、図１５に示すステップＳ３１６において機能証明書が再生制御情報ＡＣｐに対応していると判定される。

【０１５６】このように、機能証明書を備えない携帯電話機にメモリカードが装着された場合でも、デフォルト値を機能証明書として用いることによって図１５および図１６に示すフローチャートに従って暗号化コンテンツデータの再生許諾処理を実行でき、機能証明書を備えない携帯電話機においても、暗号化コンテンツデータの再生を行なうことができる。

【０１５７】実施の形態１によれば、携帯電話機は、機能証明書を備え、メモリカードは携帯電話機から送信された機能証明書が再生制御情報に対応している場合に暗号化コンテンツデータを復号および再生するライセンス鍵を携帯電話機へ出力するので、再生制御情報に制限情報を設定するだけで暗号化コンテンツデータの再生を容易に制限できる。

【０１５８】［実施の形態２］図１７を参照して、実施の形態２による携帯電話機１００Ａは、携帯電話機１００の機能証明書保持部１５０７を機能証明書保持部１５０７Ａに代えたものであり、その他は携帯電話機１００と同じである。機能証明書保持部１５０７Ａは、機能証明書Ｃｐｂ１をコンテンツ再生デバイス１５５０に固有な公開暗号鍵ＫＰｐ１によって暗号化した暗号化データ｛Ｃｐｂ１｝ＫＰｐ１の形式で機能証明書Ｃｐｂ１を保持する。

【０１５９】図１８を参照して、実施の形態２による携帯電話機１０２Ａは、携帯電話機１０２の機能証明書保持部１５０７を機能証明書保持部１５０７Ａに代えたものであり、その他は携帯電話機１０２と同じである。機能証明書保持部１５０７Ａは、機能証明書Ｃｐｂ２をコンテンツ再生デバイス１５５０に固有な公開暗号鍵ＫＰｐ１によって暗号化した暗号化データ｛Ｃｐｂ１｝ＫＰｐ１の形式で機能証明書Ｃｐｂ２を保持する。

【０１６０】このように、実施の形態２においては、携帯電話機１００Ａ，１０２Ａは、機能証明書Ｃｐｂｉをコンテンツ再生デバイス１５５０に固有な公開暗号鍵ＫＰｐ１によって署名した形式で保持する。そして、メモリカードは、暗号化データ｛Ｃｐｂ１｝ＫＰｐ１を公開暗号鍵ＫＰｐ１によって復号し、機能証明書Ｃｐｂｉを受理したか否かを判定することによって機能証明書Ｃｐｂｉを正規なコンテンツ再生デバイスから受理したことを確認できる。

【０１６１】図１９を参照して、実施の形態２によるメモリカード１１０Ａは、メモリカード１１０に復号処理部１４０９を追加したものであり、その他は、メモリカード１１０と同じである。復号処理部１４０９は、再生許諾処理において、暗号化データ｛Ｃｐｂｉ｝ＫＰｐ１を、復号処理部１４０８によって復号された公開暗号鍵ＫＰｐ１によって復号して機能証明書Ｃｐｂｉを取得する。この場合、復号処理部１４０８は、認証データ｛ＫＰｐ１／／Ｃｐａ１｝を公開認証鍵ＫＰａによって復号して得られた公開暗号鍵ＫＰｐ１を暗号処理部１４１０および復号処理部１４０９へ出力する。

【０１６２】暗号化コンテンツデータを再生する際に、携帯電話機１００Ａ，１０２Ａ，１０４とメモリカード１１０Ａとの間で行なわれる初期化処理は、図１４に示すフローチャートに従って行なわれる。また、再生許諾処理は、図２０に示すフローチャートに従って行なわれる。図２０に示すフローチャートは、図１５に示すフローチャートにおいてステップＳ３０６，Ｓ３０８，Ｓ３１０をステップＳ３０６ｂ，Ｓ３０８ｂ，Ｓ３１０ｂ，Ｓ３１０ｃ，Ｓ３１０ｄに代えたものであり、その他は図１５に示すフローチャートと同じである。

【０１６３】ステップＳ３０４の後、携帯電話機１００Ａ，１０２Ａ，１０４の暗号処理部１５０６は、機能証明書保持部１５０７Ａからの機能証明書｛Ｃｐｂｉ｝ＫＰｐ１とセッションキー発生部１５０８からのセッションキーＫｓ３とを、復号処理部１５０４からのセッションキーＫｓ２によって暗号化し、暗号化データ｛｛Ｃｐｂｉ｝ＫＰｐ１／／Ｋｓ３｝Ｋｓ２をバスＢＳ２へ出力する（ステップＳ３０６ｂ）。コントローラ１１２０は、バスＢＳ２上の暗号化データ｛｛Ｃｐｂｉ｝ＫＰｐ１／／Ｋｓ３｝Ｋｓ２をメモリカードインタフェース１２００を介してメモリカード１１０Ａへ入力する（ステップＳ３０８ｂ）。

【０１６４】そうすると、メモリカード１１０Ａにおいては、コントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介して暗号化データ｛｛Ｃｐｂｉ｝ＫＰｐ１／／Ｋｓ３｝Ｋｓ２を受取り、その受取った暗号化データ｛｛Ｃｐｂｉ｝ＫＰｐ１／／Ｋｓ３｝Ｋｓ２をバスＢＳ３を介して復号処理部１４１２に与える。そして、復号処理部１４１２は、暗号化データ｛｛Ｃｐｂｉ｝ＫＰｐ１／／Ｋｓ３｝Ｋｓ２を、セッションキー発生部１４１８からのセッションキーＫｓ２によって復号し、暗号化データ｛Ｃｐｂｉ｝ＫＰｐ１およびセッションキーＫｓ３を受理する（ステップＳ３１０ｂ）。復号処理部１４１２は、復号して得られた暗号化データ｛Ｃｐｂｉ｝ＫＰｐ１を復号処理部１４０９へ出力し、セッションキーＫｓ３をスイッチ１４４２の接点Ｐｂへ出力する。

【０１６５】そして、復号処理部１４０９は、暗号化データ｛Ｃｐｂｉ｝ＫＰｐ１を、復号処理部１４０８からの公開暗号鍵ＫＰｐ１によって復号し、機能証明書Ｃｐｂｉをバスｂｓ３へ出力する（ステップＳ３１０ｃ）。コントローラ１４２０は、機能証明書Ｃｐｂｉを受理したか否かを判定し（ステップＳ３１０ｄ）、機能証明書Ｃｐｂｉを受理しないとき、再生許諾処理は終了する（ステップＳ３３０）。ステップＳ３１０ｄにおいて、コントローラ１４２０が機能証明書Ｃｐｂｉを受理したと判定したときステップＳ３１２～Ｓ３３０が行なわれて再生許諾処理が終了する。

【０１６６】メモリカード１１０Ａが携帯電話機１０４

に装着されたとき、図２０に示すフローチャートのステップＳ３０６ｂ，Ｓ３０８ｂ，Ｓ３１０ｂ，Ｓ３１０ｃ，Ｓ３１０ｄを図１６に示すステップＳ３０６ａ，Ｓ３０８ａ，Ｓ３１０ａ，Ｓ３１１に代えたフローチャートに従って携帯電話機１０４における再生許諾処理が行なわれる。

【０１６７】その他は、実施の形態１と同じである。実施の形態２によれば、携帯電話機は、機能証明書をコンテンツ再生デバイスに固有な公開暗号鍵によって署名した形式で保持するので、公開暗号鍵を保持するメモリカードのみが機能証明書を受理することができ、不正なメモリカードが機能証明書を受理するのを防止できる。

【０１６８】［実施の形態３］図２１を参照して、実施の形態３による携帯電話機１００Ｂは、携帯電話機１００Ａの機能証明書保持部１５０７Ａを機能証明書保持部１５０７Ｂに代えたものであり、その他は携帯電話機１００Ａと同じである。機能証明書保持部１５０７Ｂは、機能証明書｛Ｃｐｂ１｝ＫＰｐ１をバスＢＳ２へ直接出力する。

【０１６９】図２２を参照して、実施の形態３による携帯電話機１０２Ｂは、携帯電話機１０２Ａの機能証明書保持部１５０７Ａを機能証明書保持部１５０７Ｂに代えたものであり、その他は携帯電話機１０２Ａと同じである。機能証明書保持部１５０７Ｂは、機能証明書｛Ｃｐｂ２｝ＫＰｐ１をバスＢＳ２へ直接出力する。

【０１７０】図２３を参照して、実施の形態３によるメモリカード１１０Ｂは、実施の形態２によるメモリカード１１０Ａと同じ構成要素から成るが、復号処理部１４１２は、セッションキーＫｓ２によって暗号化データを復号した結果を復号処理部１４０９へ出力しない点、および復号処理部１４０９は、バスＢＳ３との間でデータをやり取りする点がメモリカード１１０Ａと異なる。

【０１７１】実施の形態３によるメモリカード１１０Ｂは、携帯電話機１００Ｂ，１０２Ｂから認証データ｛ＫＰｐ１／／Ｃｐａ１｝ＫＰａと機能証明書｛Ｃｐｂｉ｝ＫＰｐ１とを初期化処理において受信することに対応したメモリカードである。

【０１７２】図２４を参照して、実施の形態３による暗号化コンテンツデータの再生処理における初期化処理について説明する。図２４に示すフローチャートは、図１４に示すフローチャートのステップＳ２０４，Ｓ２０６，Ｓ２０８をステップＳ２０４ａ，Ｓ２０６ａ，Ｓ２０８ａに代え、ステップＳ２１２とステップＳ２１４との間にステップＳ２１３ａ，Ｓ２１３ｂを挿入したものであり、その他は図１４に示すフローチャートと同じである。ステップＳ２０２の後、携帯電話機１００Ｂ，１０２Ｂのコントローラ１１２０は、コンテンツ再生デバイス１５５０の認証データ保持部１５００および機能証明書保持部１５０７Ｂへそれぞれ認証データ｛ＫＰｐ１／／Ｃｐａ１｝ＫＰａおよび機能証明書｛Ｃｐｂｉ｝ＫＰｐ１を出力するように要求し、認証データ保持部１５００は、認証データ｛ＫＰｐ１／／Ｃｐａ１｝ＫＰａをバスＢＳ２へ出力し、機能証明書保持部１５０７Ｂは、機能証明書｛Ｃｐｂｉ｝ＫＰｐ１をバスＢＳ２へ出力する（ステップＳ２０４ａ）。そして、コントローラ１１２０は、バスＢＳ２およびメモリカードインタフェース１２００を介して｛ＫＰｐ１／／Ｃｐａ１｝ＫＰａ／／｛Ｃｐｂｉ｝ＫＰｐ１をメモリカード１１０Ｂへ出力する（ステップＳ２０６ａ）。

【０１７３】そうすると、メモリカード１１０Ｂのコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介して暗号化データ｛ＫＰｐ１／／Ｃｐａ１｝ＫＰａ／／｛Ｃｐｂｉ｝ＫＰｐ１を受取る（ステップＳ２０８ａ）。その後、上述したステップＳ２１０，Ｓ２１２が実行される。そして、コントローラ１４２０は、暗号化データ｛Ｃｐｂｉ｝ＫＰｐ１を復号処理部１４０９に与え、復号処理部１４０９は、暗号化データ｛Ｃｐｂｉ｝ＫＰｐ１を復号処理部１４０８からの公開暗号鍵ＫＰｐ１によって復号し（ステップＳ２１３ａ）、機能証明書ＣｐｂｉをバスＢＳ３へ出力する。コントローラ１４２０は、機能証明書Ｃｐｂｉを受理したか否かを判定し（ステップＳ２１３ｂ）、機能証明書Ｃｐｂｉを受理しなかったとき初期化処理が終了する（ステップＳ２２２）。ステップＳ２１３ｂにおいてコントローラ１４２０が機能証明書Ｃｐｂｉを受理したと判定したとき上述したステップＳ２１４～Ｓ２２０が実行されて初期化処理が終了する。

【０１７４】図２５を参照して、メモリカード１１０Ｂが携帯電話機１０４に装着された場合の初期化処理について説明する。図２５に示すフローチャートは図１４に示すフローチャートのステップＳ２１２とステップＳ２１４との間にステップＳ２１３，Ｓ２１３ｂを挿入したものであり、その他は図１４に示すフローチャートと同じである。

【０１７５】ステップＳ２１２において、メモリカード１１０Ｂのコントローラ１４２０は、公開暗号鍵ＫＰｐ１を受理したと判定すると、デフォルト値を携帯電話機１０４のコンテンツ再生デバイス１５５０の機能証明書Ｃｐｂｉとして受理する（ステップＳ２１３）。そして、コントローラ１４２０は、機能証明書Ｃｐｂｉを受理したか否かを判定し（ステップＳ２１３ｂ）、機能証明書Ｃｐｂｉを受理しなかったとき初期化処理が終了する（ステップＳ２２２）。ステップＳ２１３ｂにおいてコントローラ１４２０が機能証明書Ｃｐｂｉを受理したと判定したとき上述したステップＳ２１４～Ｓ２２０が実行されて初期化処理が終了する。ステップＳ２１３においてデフォルト値を機能証明書Ｃｐｂｉとして受理しているのでコントローラ１４２０は、ステップＳ２１３ｂにおいて機能証明書Ｃｐｂｉを受理したと判定する。

【０１７６】このように、メモリカードが機能証明書を

備えない携帯電話機に装着された場合でも、初期化処理が実行されて暗号化コンテンツデータの再生が行なわれる。

【０１７７】図２６を参照して、実施の形態３における再生許諾処理の動作について説明する。図２６に示すフローチャートは、図１５に示すフローチャートのステップＳ３０６，Ｓ３０８，Ｓ３１０をステップＳ３０６ａ，Ｓ３０８ａ，Ｓ３１０ａに代えたものであり、その他は図１５に示すフローチャートと同じである。ステップＳ３０４の後、携帯電話機１００Ｂ，１０２Ｂ，１０４の暗号処理部１５０６は、セッションキー発生部１５０８からのセッションキーＫｓ３を、復号処理部１５０４からのセッションキーＫｓ２によって暗号化して暗号化データ｛Ｋｓ３｝Ｋｓ２をバスＢＳ２へ出力する（ステップＳ３０６ａ）。そして、コントローラ１１２０は、暗号化データ｛Ｋｓ３｝Ｋｓ２をバスＢＳ２を介して受理し、メモリカードインタフェース１２００を介してメモリカード１１０Ｂへ出力する（ステップＳ３０８ａ）。そうすると、メモリカード１１０Ｂのコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ３を介して暗号化データ｛Ｋｓ３｝Ｋｓ２を受取り、その受取った暗号化データ｛Ｋｓ３｝Ｋｓ２をバスＢＳ３を介して復号処理部１４１２に与える。復号処理部１４１２は、暗号化データ｛Ｋｓ３｝Ｋｓ２を、セッションキー発生部１４１８からのセッションキーＫｓ２によって復号してセッションキーＫｓ３を受理する（ステップＳ３１０ａ）。その後、ステップ３１２～Ｓ３２８が実行されて再生許諾処理が終了する（ステップＳ３３０）。

【０１７８】その他は、実施の形態１と同じである。実施の形態３によれば、暗号化コンテンツデータの再生処理における初期化処理において認証データと機能証明書とが携帯電話機からメモリカードへ送信されるので、携帯電話機の機能を１回確認すれば、以後、携帯電話機の機能を確認しなくても暗号化コンテンツデータを再生できる。

【０１７９】上記においては、フラグＦＧ１，ＦＧ２に関しては機能証明に記載されないものとして説明したが、フラグＦＧ１は再生速度変更禁止を示すことから、再生速度を変更することができないコンテンツ再生デバイスや再生速度を変更することができるがフラグＦＧ１がアクティブ「１」の場合に変更を行なわないように制御できるコンテンツ再生デバイスに対する機能証明書は対応可能であるとして記載され、コンテンツ再生デバイスはフラグＦＧ１がアクティブ「１」であるときには必ず指定の速度で再生する。

【０１８０】また、フラグＦＧ２は編集可否であることから、フラグＦＧ２がアクティブ「１」の場合には特殊再生に用いることが禁止されるため、フラグＦＧ２に従って特殊再生に帰依しないように再生を行なうことが可能なコンテンツ再生デバイスに対する機能証明書は対応可能であるとして記載され、コンテンツ再生デバイスは、フラグＦＧ２がアクティブ「１」のコンテンツを特殊再生時には再生しないように制御することで機能証明に追加することも可能である。

【０１８１】さらに、コンテンツ再生デバイスの標準機能を予め定めた上で、未対応の機能がある場合には、機能証明書に対して機能しない旨を機能証明書に記載することも可能である。

【０１８２】また、さらに、機能証明書に対して再生制限フラグを構成する各フラグと一意に対応するフラグによって構成される対応機能フラグを設けて機能を記載することもでき、この場合にはステップＳ３１６における判断は、再生制限フラグと再生機能対応フラグとの位置を確認すればよい。

【０１８３】実施の形態１～実施の形態３においては、携帯電話機に備えられたメモリカードに対してコンテンツデータとして音楽データをダウンロードして記録し、携帯電話機に備えられたコンテンツ再生デバイスによってメモリカードに記録された音楽データを再生するように説明したが、本発明は、これに限定されるものではない。

【０１８４】本発明は、音楽データのみならず、画像データ、動画データ、テキストデータ、朗読データ、音源データ、およびゲーム等のアプリケーションプログラム等に対応可能であり、著作権者あるいはデータの権利者の権利を守る必要があるデータ全般に適用可能である。

【０１８５】また、携帯電話網を介してライセンスをダウンロードするように説明したが、データの供給源を規定するものではなく、インターネット等のデジタル通信網に対しても適用可能である。さらに、パーソナルコンピュータなどの機器でメモリカードに、直接、書込むことも可能である。

【０１８６】さらに、ライセンスを記録する記録装置としてメモリカードを例に挙げで説明したが、メモリカードに限定するものではなく、ハードディスクなどの入出力の制御を行なえる記録装置であれば、いかなる媒体であってもかまわない。

【０１８７】また、さらに、ライセンスと暗号化コンテンツデータは、必ずしも同一の記録装置上に記録される必要はなく、暗号化コンテンツデータは従来の記録装置に記録されていてもかまわない。

【０１８８】また、さらに、コンテンツ再生デバイスは、携帯電話機に備えられているように説明したが、携帯電話機は必ずしも必要ではない。そして、配信サーバに接続してダウンロードする機能を同一端末が持つ必要はなく、記録装置（メモリカード）は、ライセンスを記録するためのダウンロード端末と、記録装置（メモリカード）から暗号化コンテンツデータとライセンスとを取得して再生するコンテンツ再生デバイスを備える再生端

末とから構成されていてもよい。

【０１８９】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【０１９０】

【発明の効果】本発明によれば、携帯電話機は、機能証明書を備え、メモリカードは携帯電話機から送信された機能証明書が再生制御情報に対応している場合に暗号化コンテンツデータを復号および再生するライセンス鍵を携帯電話機へ出力するので、再生制御情報に制限情報を設定するだけで暗号化コンテンツデータの再生を容易に制限できる。

【図面の簡単な説明】

【図１】　データ配信システムを概念的に説明する概略図である。

【図２】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図３】　図２に示す再生制御情報のフォーマットを示す図である。

【図４】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図５】　図１に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図６】　実施の形態１による携帯電話機の構成を示す概略ブロック図である。

【図７】　実施の形態１による他の携帯電話機の構成を示す概略ブロック図である。

【図８】　実施の形態１によるさらに他の携帯電話機の構成を示す概略ブロック図である。

【図９】　図１に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図１０】　図１に示すデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

【図１１】　図１に示すデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

【図１２】　メモリカードにおける再生リストファイルの構成を示す図である。

【図１３】　携帯電話機における暗号化コンテンツデータの再生動作を説明するためのフローチャートである。

【図１４】　図１３に示す実施の形態１における初期化処理の動作を説明するためのフローチャートである。

【図１５】　図１３に示す実施の形態１における再生許諾処理の動作を説明するためのフローチャートである。

【図１６】　図１５に示すフローチャートの一部を差替えるためのフローを示すフローチャートである。

【図１７】　実施の形態２による携帯電話機の構成を示す概略ブロック図である。

【図１８】　実施の形態２による他の携帯電話機の構成を示す概略ブロック図である。

【図１９】　実施の形態２によるメモリカードの構成を示す概略ブロック図である。

【図２０】　実施の形態２における再生許諾処理の動作を説明するためのフローチャートである。

【図２１】　実施の形態３による携帯電話機の構成を示す概略ブロック図である。

【図２２】　実施の形態３による他の携帯電話機の構成を示す概略ブロック図である。

【図２３】　実施の形態３によるメモリカードの構成を示す概略ブロック図である。

【図２４】　実施の形態３における初期化処理の動作を説明するためのフローチャートである。

【図２５】　実施の形態３における初期化処理の動作を説明するための他のフローチャートである。

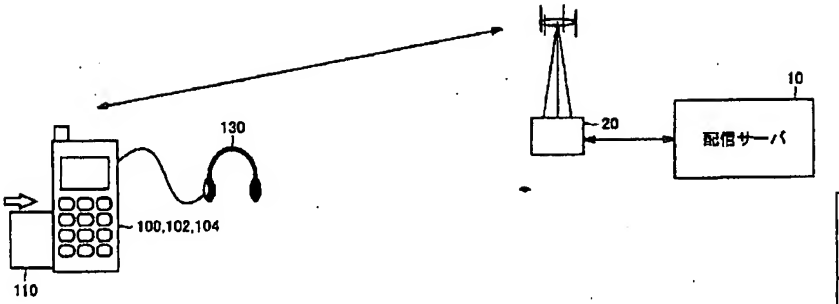
【図２６】　実施の形態３における再生許諾処理の動作を説明するためのフローチャートである。

【符号の説明】

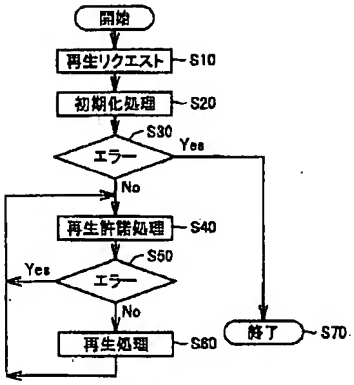
１０　配信サーバ、２０　配信キャリア、１，２，２１～２３　領域、１００，１０２，１０４，１００Ａ，１０２Ａ，１００Ｂ，１０２Ｂ　携帯電話機、１１０，１１０Ａ，１１０Ｂ　メモリカード、１３０　ヘッドホーン、１６０　再生リストファイル、１６５　エントリ管理情報、３０２　課金データベース、３０４　情報データベース、３０７　メニューデータベース、３０８　配信記録データベース、３１０　データ処理部、３１２，３２０，１４０４，１４０８，１４０９，１４１２，１４２２，１５０４，１５１０，１５１６　復号処理部、３１３　認証鍵保持部、３１５　配信制御部、３１６，１４１８，１５０８　セッションキー発生部、３１８，３２６，３２８，１４０６，１４１０，１５０６暗号処理部、３５０　通信装置、１１２０，１４２０　コントローラ、１４２６，１５３０　端子、１１００　アンテナ、１１０２　送受信部、１１０４　マイク、１１０６　ＡＤ変換部、１１０８　音声符号化部、１１１０　音声再生部、１１１２，１５１９　ＤＡ変換部、１１１４　スピーカ、１１１６　操作パネル、１１１８　表示パネル、１２００　メモリカードインタフェース、１４００，１５００　認証データ保持部、１４０２　Ｋｍｃ保持部、１４１４　ＫＰａ保持部、１４１５　メモリ、１４１５Ａ　ライセンス領域、１４１５Ｂ　データ領域、１４１６　ＫＰｍｃ保持部、１４２１　Ｋｍ保持部、１４２４　インタフェース、１４４２，１４４６　切換スイッチ、１５０２　Ｋｐ保持部、１５０７，１５０７Ａ，１５０７Ｂ　機能証明書保持部、１５１２　時計、１５１４　再生制御部、１５１８　音楽再生部、１５２１～１５２５，１６２１～１６２ｎ　ライセンス管理ファイル、１５３１～１５３５，１６１１～１６１ｎ　コンテンツファイル、１５５０　コンテンツ再生デバイ

ス。

【図１】



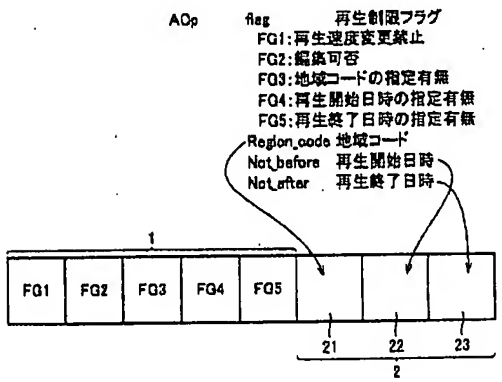
【図１３】



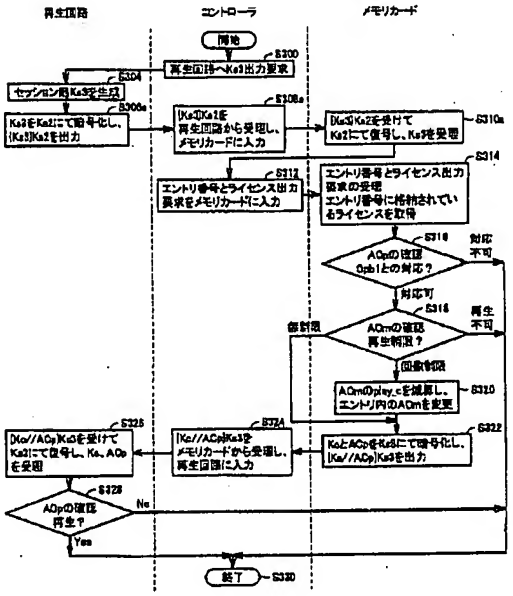
【図２】

記号	種類	属性	特性
Do	コンテンツデータ	コンテンツ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ [Dc]Kcとして配信され、メモリカードに保持される
Dc-inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス 暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンスID	ライセンス	ライセンス固有	ライセンスを特定するための管理コード
ライセンス	ライセンス	ライセンス固有	Kc＋ACm＋ACp＋コンテンツID＋ライセンスIDの総称

【図３】



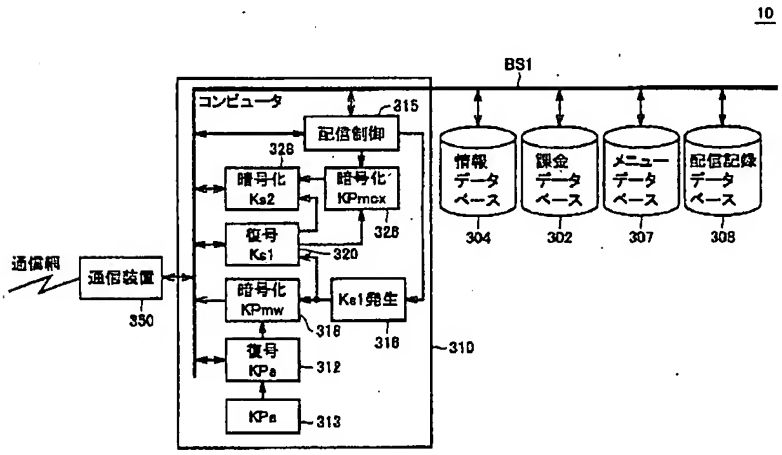
【図２６】



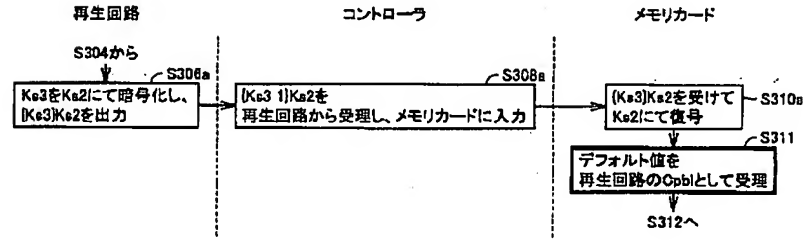
【図４】

	記号	種類	属性	特性
配信サーバ	KPa	公開認証鍵	システム共通	認証局にて認証データを復号する鍵
	Ks1	共通鍵	セッション固有	メモリカードへのライセンス配信ごとに発生
メモリカード	KPa	公開認証鍵	システム共通	認証局にて認証データを復号する鍵 配信サーバのKPaと同一
	KPmw	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
	Kmw	秘密復号鍵	クラス固有	公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な復号鍵
	KPmcx	公開暗号鍵	個別	メモリカードごとに異なる。 xはモジュールを識別するための識別子
	Kmcx	秘密復号鍵	個別	公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な復号鍵
	Ks2	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間のライセンスの授受ごとに発生
	Cmw	証明書	クラス証明書	メモリカードのクラス証明書。 認証機能を有する。 {KPmw//Cmw}KPaの形式で出荷時に記録。 ＊メモリカードのクラスwごとに異なる。
コンテンツ再生デバイス	KPpy	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
	Kpy	秘密復号鍵	クラス固有	公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵
	Ks3	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間の再生セッションごとに発生
	Opay	証明書	クラス証明書	コンテンツ再生デバイスのクラス証明書。認証機能を有する。 {KPpy//Opay}KPaの形式で出荷時に記録。 ＊コンテンツ再生デバイスのクラスyごとに異なる。
	Opbl	証明書	機能証明書	コンテンツ再生デバイスの機能証明書。 OpblまたはにOpbl}KPpyの形式で出荷時に記録。 ＊コンテンツ再生デバイスのクラスxごとに異なる。

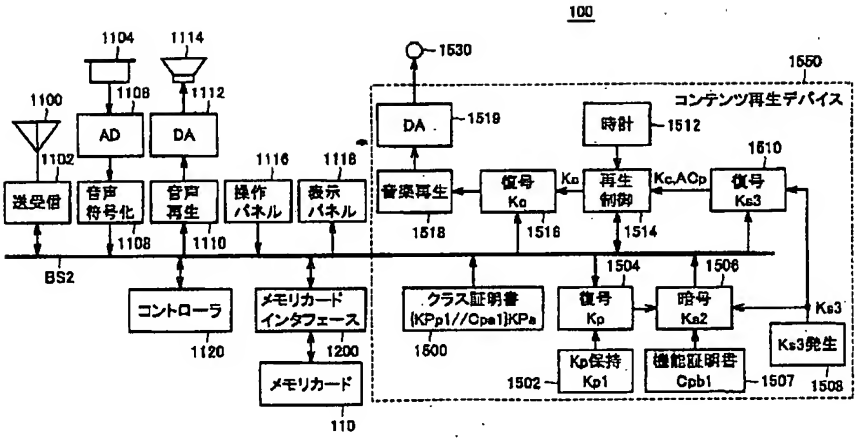
【図５】



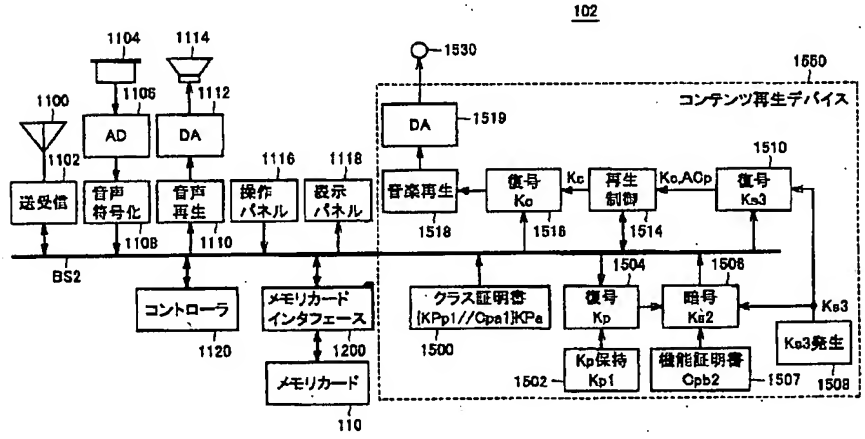
【図１６】



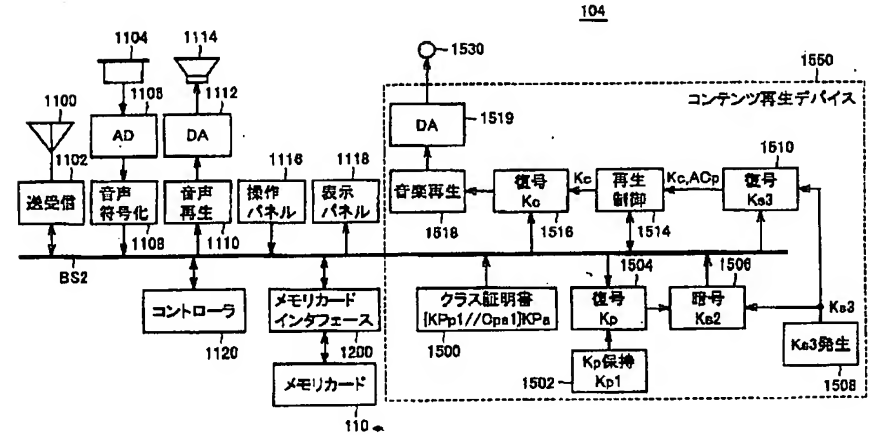
【図６】


100
1104
1114
1530
1550
コンテンツ再生デバイス
1100
1108
1112
AD
DA
DA
1519
時計
1512
1610
1102
1116
1118
送受信
音声符号化
音声再生
操作パネル
表示パネル
音楽再生
復号 Ko
Ko
再生制御
Kc,ACp
復号 Ks3
1108
1110
1518
1516
1514
1504
1506
BS2
コントローラ
メモリカードインタフェース
クラス証明書 [KPp1//Cpa1]KPa
復号 Kp
暗号 Ks2
Ks3
Ks3発生
1120
1200
1500
Kp保持 Kp1
機能証明書 Cpb1
1502
1507
1508
メモリカード
110

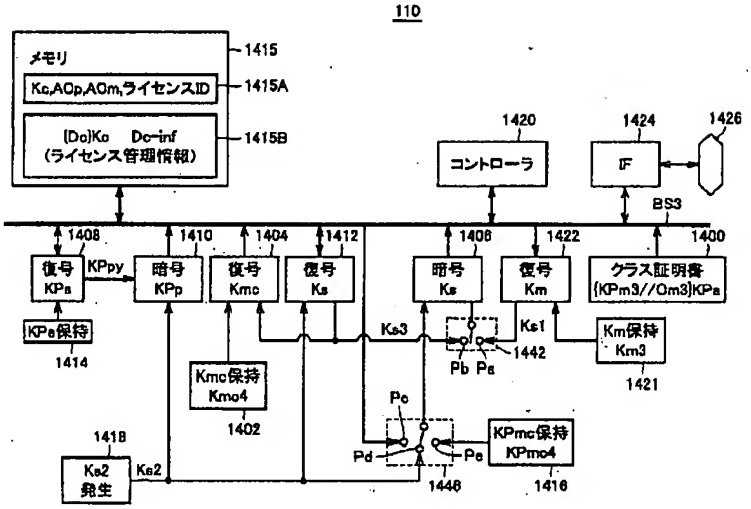
【図７】


102
1104
1114
1530
1550
コンテンツ再生デバイス
1100
1106
1112
AD
DA
DA
1519
1510
1102
1116
1118
送受信
音声符号化
音声再生
操作パネル
表示パネル
音楽再生
復号 Ko
Ko
再生制御
Kc,ACp
復号 Ks3
1108
1110
1518
1516
1514
1504
1506
BS2
コントローラ
メモリカードインタフェース
クラス証明書 [KPp1//Cpa1]KPa
復号 Kp
暗号 Ks2
Ks3
Ks3発生
1120
1200
1500
Kp保持 Kp1
機能証明書 Cpb2
1502
1507
1508
メモリカード
110

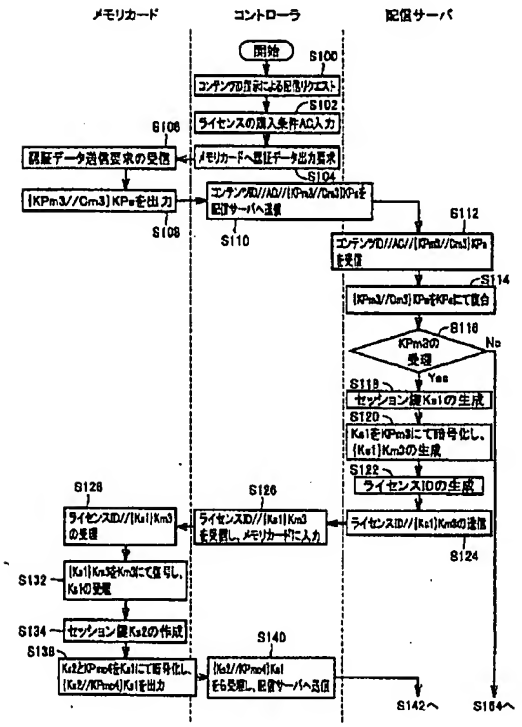
【図８】


104
1104
1114
1530
1550
コンテンツ再生デバイス
1100
1108
1112
AD
DA
DA
1519
1610
1102
1116
1118
送受信
音声符号化
音声再生
操作パネル
表示パネル
音楽再生
復号 Ko
Ko
再生制御
Kc,ACp
復号 Ks3
1108
1110
1518
1516
1514
1504
1506
BS2
コントローラ
メモリカードインタフェース
クラス証明書 [KPp1//Cpa1]KPa
復号 Kp
暗号 Ks2
Ks3
Ks3発生
1120
1200
1500
Kp保持 Kp1
1502
1508
メモリカード
110

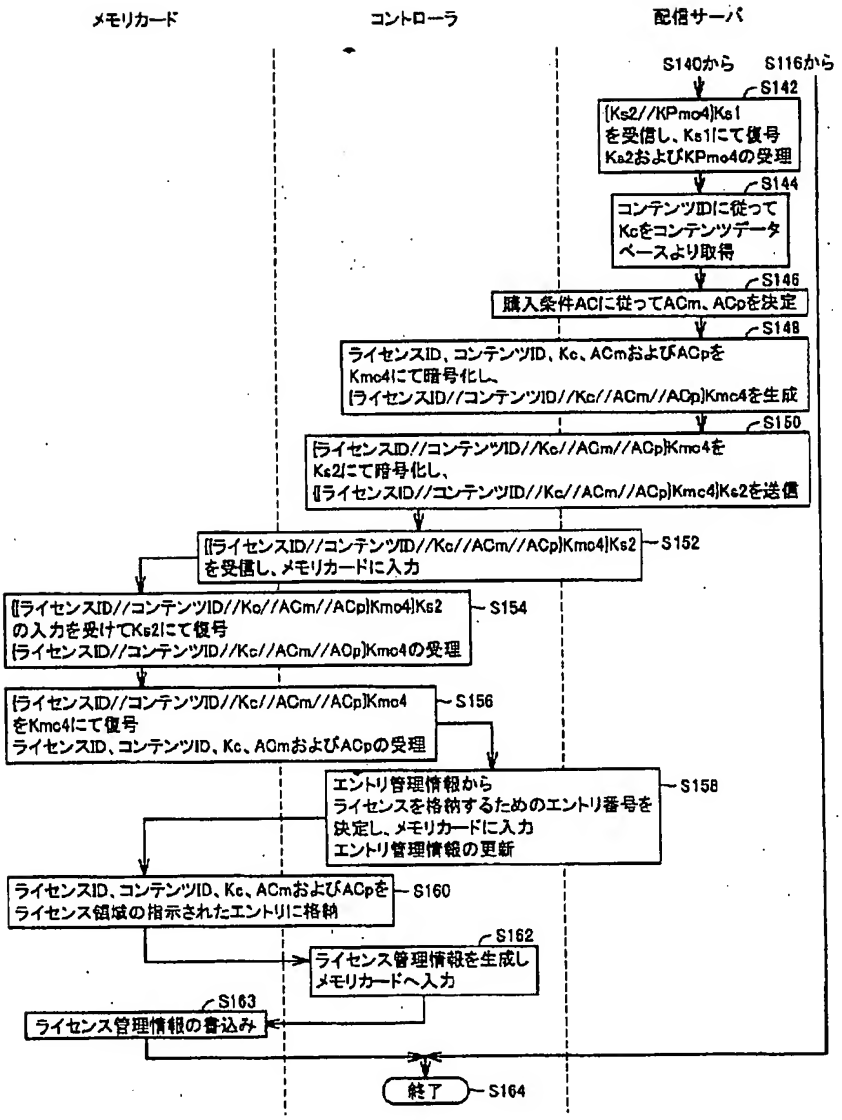
【図９】


110
メモリ
1415
Kc,AOp,AOm,ライセンスID
1415A
(Dc)Ko Dc-inf
(ライセンス管理情報)
1415B
コントローラ
1420
IF
1424
1426
BS3
1408
1410
1404
1412
1406
1422
1400
復号 KPs
KPpy
暗号 KPp
復号 Kmc
復号 Ks
暗号 Ks
復号 Km
クラス証明書 (KPm3//Cm3)KPs
KPs保持
1414
Ks3
Ks1
1442
Pb Ps
Km保持 Km3
1421
Kmc保持 Kmc4
1402
Pc
1418
Ks2 発生
Ks2
Pd
Pe
1448
KPmc保持 KPmc4
1416

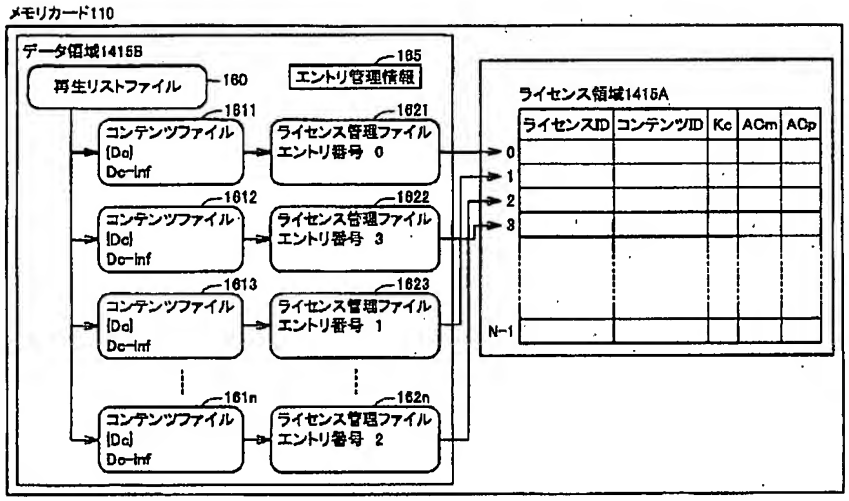
【図１０】


メモリカード
コントローラ
配信サーバ
開始
S100
コンテンツの指示による配信リクエスト
S102
ライセンスの購入条件ACを入力
S106
認証データ送信要求の受信
メモリカードへ認証データ出力要求
S104
(KPm3//Cm3)KPsを出力
S108
コンテンツID//AC//(KPm3//Cm3)KPsを配信サーバへ送信
S110
S112
コンテンツID//AC//(KPm3//Cm3)KPsを受信
S114
(KPm3//Cm3)KPsをKPsにて復合
S116
KPm3の受理
No
Yes
S118
セッション鍵Ks1の生成
S120
Ks1をKPm3にて暗号化し、(Ks1|Km3)の生成
S122
ライセンスIDの生成
S124
ライセンスID//(Ks1|Km3)の送信
S126
ライセンスID//(Ks1|Km3)を受信し、メモリカードに入力
S128
ライセンスID//(Ks1|Km3)の生成
S132
(Ks1|Km3)をKm3にて復号し、Ks1の抽出
S134
セッション鍵Ks2の作成
S138
Ks2とKPmc4をKs1にて暗号化し、(Ks2//KPmc4)Ks1を出力
S140
(Ks2//KPmc4)Ks1をS5受信し、配信サーバへ送信
S142へ
S154へ

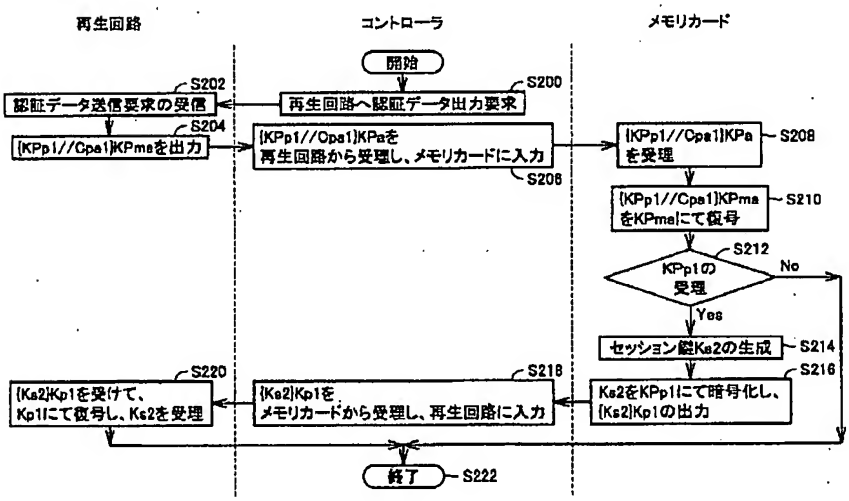
【図１１】


メモリカード
コントローラ
配信サーバ
S140から
S116から
S142
{Ks2//KPmc4}Ks1
を受信し、Ks1にて復号
Ks2およびKPmc4の受理
S144
コンテンツIDに従って
Kcをコンテンツデータ
ベースより取得
S146
購入条件ACに従ってACm、ACpを決定
S148
ライセンスID、コンテンツID、Kc、ACmおよびACpを
Kmc4にて暗号化し、
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を生成
S150
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を
Ks2にて暗号化し、
{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2を送信
{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2
を受信し、メモリカードに入力
S152
{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2
の入力を受けてKs2にて復号
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4の受理
S154
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4
をKmc4にて復号
ライセンスID、コンテンツID、Kc、ACmおよびACpの受理
S156
エントリ管理情報から
ライセンスを格納するためのエントリ番号を
決定し、メモリカードに入力
エントリ管理情報の更新
S158
ライセンスID、コンテンツID、Kc、ACmおよびACpを
ライセンス領域の指示されたエントリに格納
S160
S162
ライセンス管理情報を生成し
メモリカードへ入力
S163
ライセンス管理情報の書込み
終了
S164

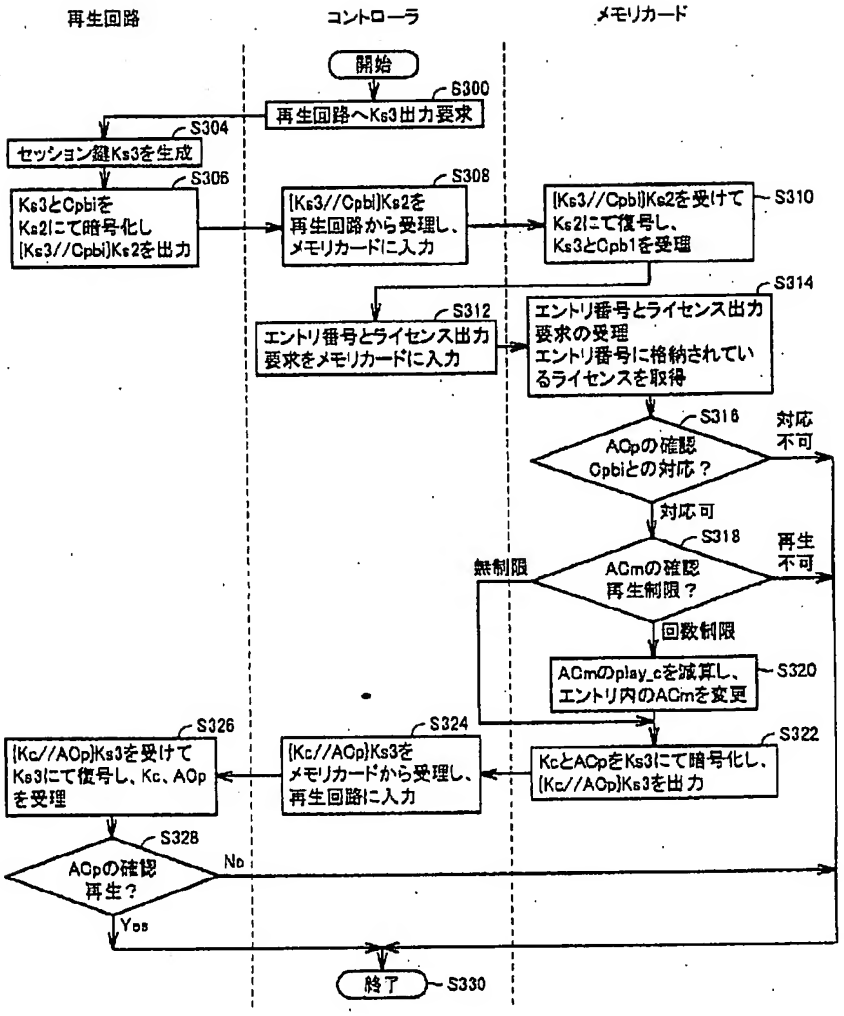
【図１２】


メモリカード110
データ領域1415B
再生リストファイル
160
エントリ管理情報
165
コンテンツファイル
[Dc]
Dc-inf
1611
1612
1613
161n
ライセンス管理ファイル
エントリ番号 0
エントリ番号 3
エントリ番号 1
エントリ番号 2
1621
1622
1623
162n
ライセンス領域1415A
ライセンスID
コンテンツID
Kc
ACm
ACp
0
1
2
3
N-1

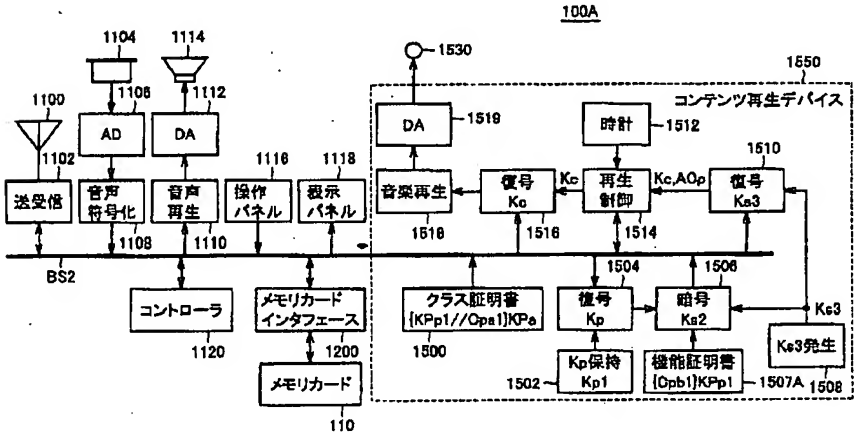
【図１４】


再生回路
コントローラ
メモリカード
開始
S200
再生回路へ認証データ出力要求
S202
認証データ送信要求の受信
S204
[KPp1//Cps1]KPmsを出力
[KPp1//Cps1]KPsを
再生回路から受理し、メモリカードに入力
S206
[KPp1//Cps1]KPs
を受理
S208
[KPp1//Cps1]KPms
をKPmsにて復号
S210
S212
KPp1の
受理
No
Yes
セッション鍵Ks2の生成
S214
Ks2をKPp1にて暗号化し、
[Ks2]Kp1の出力
S216
[Ks2]Kp1を
メモリカードから受理し、再生回路に入力
S218
[Ks2]Kp1を受けて、
Kp1にて復号し、Ks2を受理
S220
終了
S222

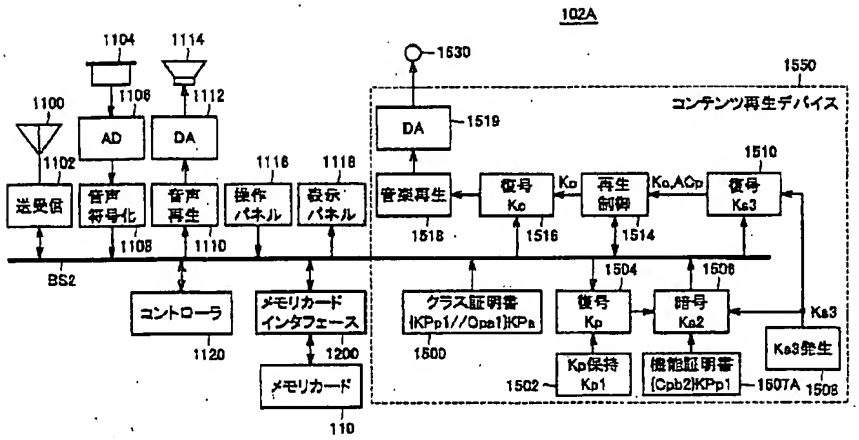
【図１５】


再生回路
コントローラ
メモリカード
開始
S300
再生回路へKs3出力要求
S304
セッション鍵Ks3を生成
S306
Ks3とCpbiを
Ks2にて暗号化し
[Ks3//Cpbi]Ks2を出力
S308
[Ks3//Cpbi]Ks2を
再生回路から受理し、
メモリカードに入力
S310
[Ks3//Cpbi]Ks2を受けて
Ks2にて復号し、
Ks3とCpb1を受理
S312
エントリ番号とライセンス出力
要求をメモリカードに入力
S314
エントリ番号とライセンス出力
要求の受理
エントリ番号に格納されてい
るライセンスを取得
S316
ACpの確認
Cpbiとの対応？
対応
不可
対応可
S318
ACmの確認
再生制限？
再生
不可
無制限
回数制限
ACmのplay_cを減算し、
エントリ内のACmを変更
S320
S322
KcとACpをKs3にて暗号化し、
[Kc//ACp]Ks3を出力
S324
[Kc//ACp]Ks3を
メモリカードから受理し、
再生回路に入力
S326
[Kc//ACp]Ks3を受けて
Ks3にて復号し、Kc、ACp
を受理
S328
ACpの確認
再生？
No
Yes
終了
S330

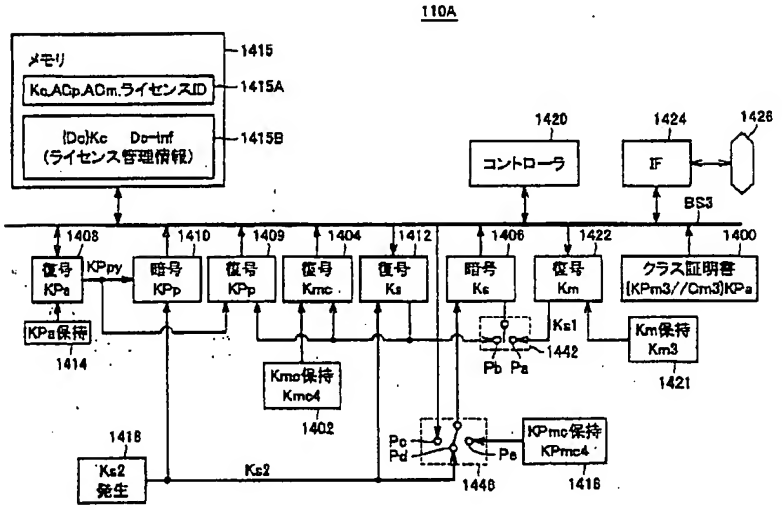
【図１７】


100A
1104
1114
1106
1112
1100
AD
DA
1102
送受信
音声
符号化
音声
再生
操作
パネル
表示
パネル
1116
1118
1108
1110
BS2
コントローラ
1120
メモリカード
インタフェース
1200
メモリカード
110
1530
1550
コンテンツ再生デバイス
DA
1519
時計
1512
1510
音楽再生
1518
復号
Kc
1516
Kc
再生
制御
1514
Kc,ACp
復号
Ks3
1504
1506
クラス証明書
[KPp1//Cps1]KPs
1500
復号
Kp
暗号
Ks2
Ks3
Ks3発生
1508
Kp保持
Kp1
1502
機能証明書
[Cpb1]KPp1
1507A

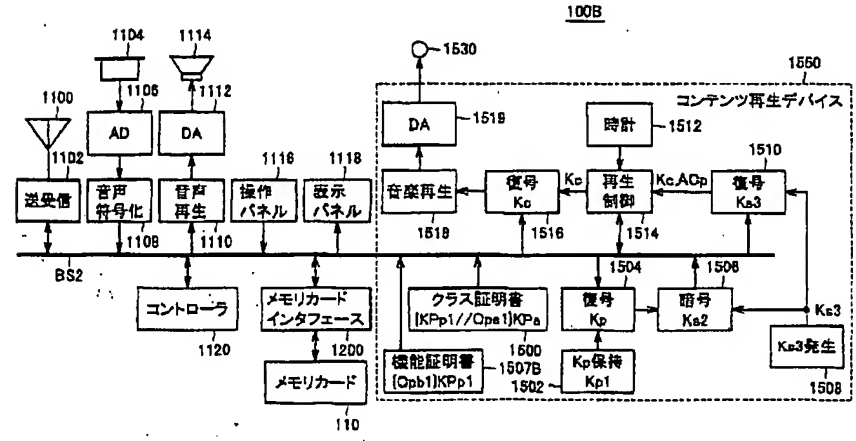
【図１８】


102A
1104
1114
1530
1550
コンテンツ再生デバイス
1100
1106
1112
AD
DA
1519
1102
1116
1118
1510
送受信
音声符号化
音声再生
操作パネル
表示パネル
音楽再生
復号 Ko
Ko
再生制御
Ko,ACp
復号 Ks3
1518
1516
1514
1108
1110
BS2
1504
1506
コントローラ
メモリカードインタフェース
クラス証明書 [KPp1//Cpa1]KPa
復号 Kp
暗号 Ks2
Ks3
1120
1200
1500
Ks3発生
メモリカード
Kp保持 Kp1
機能証明書 [Cpb2]KPp1
1502
150TA
1508
110

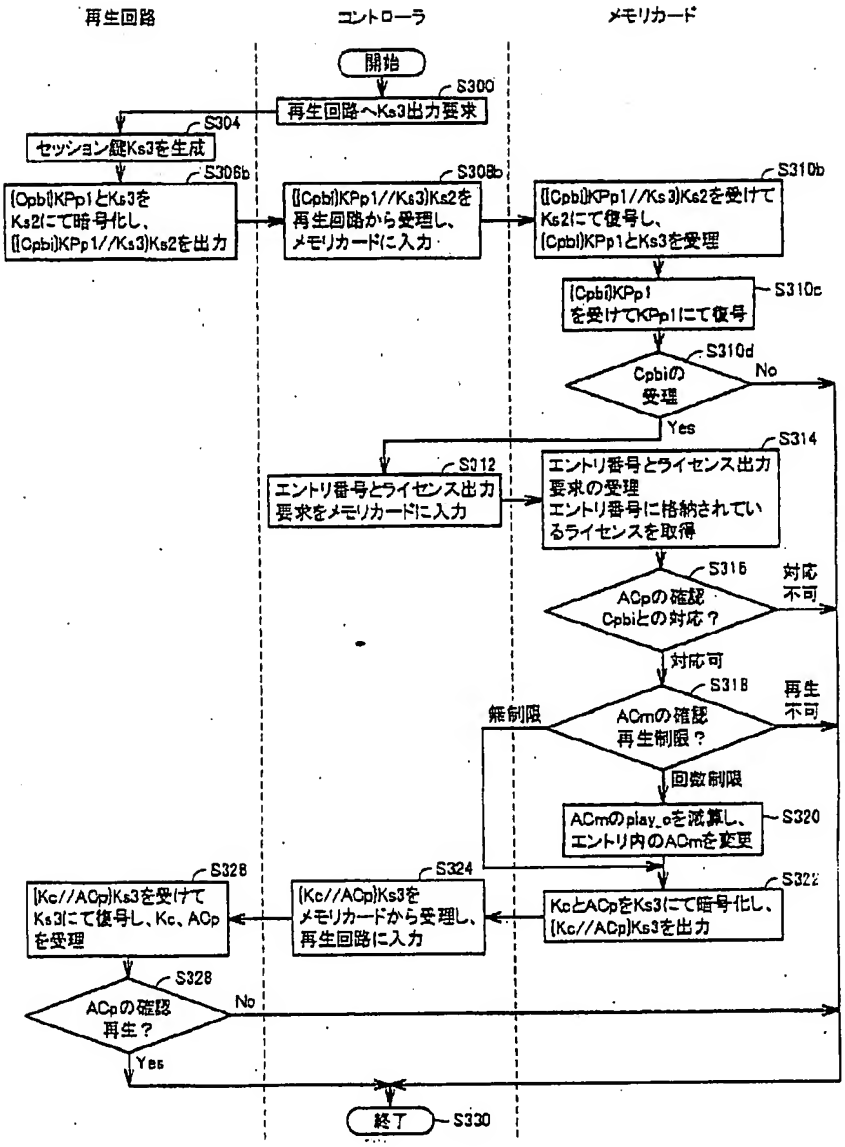
【図１９】


110A
メモリ
1415
Kc,ACp,ACm,ライセンスID
1415A
[Dc]Kc Dc-Inf
(ライセンス管理情報)
1415B
1420
1424
1428
コントローラ
IF
BS3
1408
1410
1409
1404
1412
1406
1422
1400
復号 KPa
KPpy
暗号 KPp
復号 KPp
復号 Kmc
復号 Ks
暗号 Ks
復号 Km
クラス証明書 [KPm3//Cm3]KPa
KPa保持
1414
Ks1
1442
Pb Pa
Km保持 Km3
1421
Kmc保持 Kmc4
1402
1418
Pc Pd
Pa
KPmc保持 KPmc4
Ks2 発生
Ks2
1448
1416

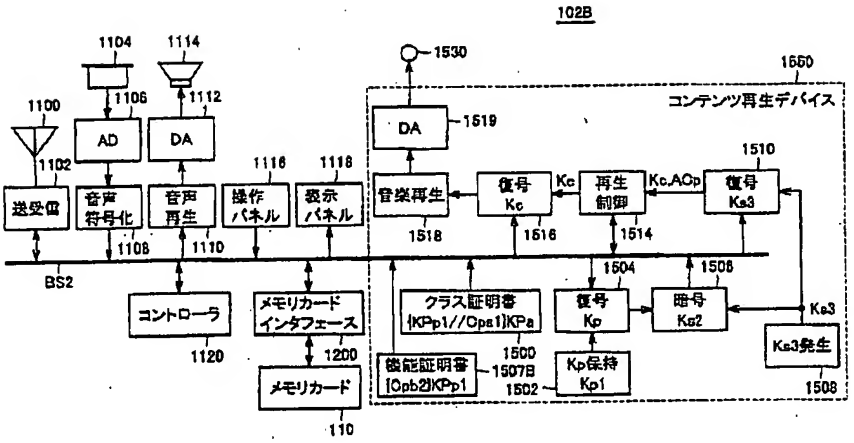
【図２１】


100B
1104
1114
1530
1550
コンテンツ再生デバイス
1100
1106
1112
AD
DA
1519
時計
1512
1102
1116
1118
1510
送受信
音声符号化
音声再生
操作パネル
表示パネル
音楽再生
復号 Ko
Ko
再生制御
Kc,ACp
復号 Ks3
1518
1516
1514
1108
1110
BS2
1504
1506
コントローラ
メモリカードインタフェース
クラス証明書 [KPp1//Cpa1]KPa
復号 Kp
暗号 Ks2
Ks3
1120
1200
1500
Ks3発生
機能証明書 [Cpb1]KPp1
1507B
Kp保持 Kp1
1502
1508
メモリカード
110

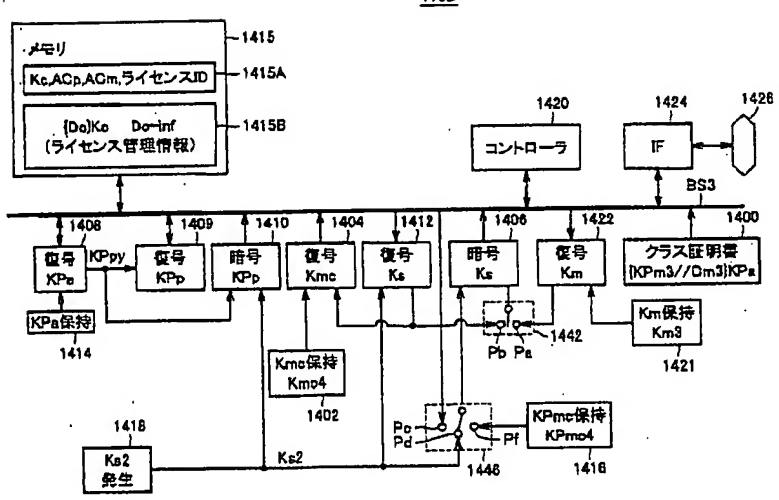
【図２０】


再生回路
コントローラ
メモリカード
開始
S300
再生回路へKs3出力要求
S304
セッション鍵Ks3を生成
S306b
{Cpbi||KPp1とKs3をKs2にて暗号化し、{||Cpbi||KPp1//Ks3)Ks2を出力
S308b
{||Cpbi||KPp1//Ks3)Ks2を再生回路から受理し、メモリカードに入力
S310b
{||Cpbi||KPp1//Ks3)Ks2を受けてKs2にて復号し、{Cpbi||KPp1とKs3を受理
{Cpbi||KPp1を受けてKPp1にて復号
S310c
S310d
Cpbiの受理
No
Yes
S312
エントリ番号とライセンス出力要求をメモリカードに入力
S314
エントリ番号とライセンス出力要求の受理
エントリ番号に格納されているライセンスを取得
S316
ACpの確認
Cpbiとの対応？
対応不可
対応可
S318
ACmの確認
再生制限？
再生不可
無制限
回数制限
ACmのplay_cを減算し、エントリ内のACmを変更
S320
S322
KcとACpをKs3にて暗号化し、{Kc//ACp}Ks3を出力
S324
{Kc//ACp}Ks3をメモリカードから受理し、再生回路に入力
S326
{Kc//ACp}Ks3を受けてKs3にて復号し、Kc、ACpを受理
S328
ACpの確認
再生？
No
Yes
終了
S330

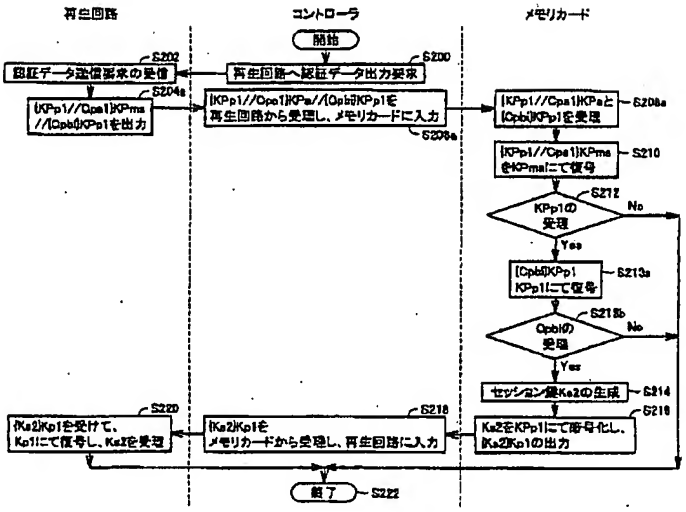
【図２２】


102B
1104
1114
1530
1550
コンテンツ再生デバイス
1100
1106
1112
AD
DA
DA
1519
1102
1116
1118
1510
送受信
音声符号化
音声再生
操作パネル
表示パネル
音楽再生
復号 Kc
再生制御
復号 Ks3
Kc
Kc,ACp
1108
1110
1518
1516
1514
1504
1506
BS2
コントローラ
メモリカードインタフェース
クラス証明書 [KPp1//Cps1]KPa
復号 Kp
暗号 Ks2
Ks3
Ks3発生
1120
1200
1500
機能証明書 [Cpb2]KPp1
1507B
Kp保持 Kp1
1502
1508
メモリカード
110

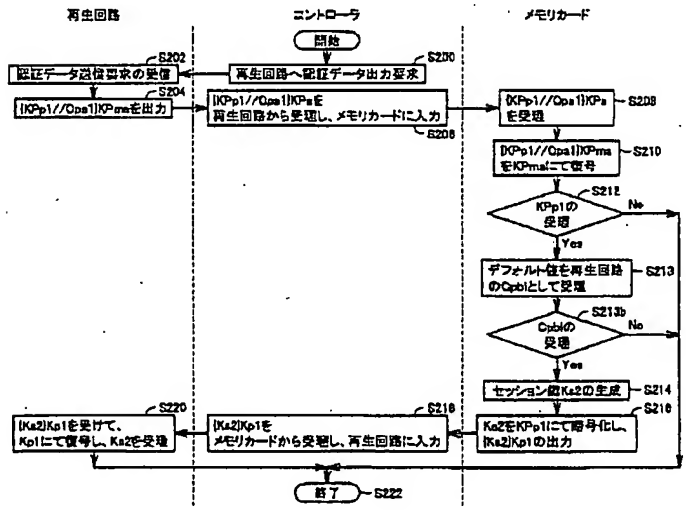
【図２３】


110B
メモリ
1415
Kc,ACp,ACm,ライセンスID
1415A
{Do}Ko Do-inf
(ライセンス管理情報)
1415B
1420
1424
1426
コントローラ
IF
BS3
1408
1409
1410
1404
1412
1406
1422
1400
復号 KPa
KPpy
復号 KPp
暗号 KPp
復号 Kmc
復号 Ks
暗号 Ks
復号 Km
クラス証明書 [KPm3//Cm3]KPa
KPa保持
1414
Km保持 Km3
1421
Pb Pa
1442
Kmc保持 Kmp4
1402
1418
Ks2 発生
Ks2
Pc Pd
Pf
KPmc保持 KPmc4
1446
1416

【図２４】



【図２５】



フロントページの続き

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
H04N 7/167		H04N	7/167	Z 5J104
// H04N 5/765		H04L	9/00	601B 5K101
5/907		H04N	5/91	L
5/91				P

Fターム(参考) 5B017 AA07 BA07 BB10 CA16
5B035 AA13 BB09 BC00 CA11 CA38
5C052 GA08 GB01 GB07 GC00 GE08
5C053 FA13 FA27 GB40 LA15
5C064 BA01 BB01 BC04 BC23 BC25
BD02 CB01 CC04
5J104 AA01 AA16 EA01 EA04 EA22
NA02 PA14
5K101 KK18 LL01 LL11